SEGURIDAD INFORMÁTICA EN EL SISTEMA OPERATIVO LINUX EN SUS DIVERSAS DISTRIBUCIONES APLICADAS A LAS TECNOLOGÍAS DE LA INFORMACIÓN

YEIMAR ALONSO CASTRO MATURANA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA (ECBTI)
TURBO, COLOMBIA
2021

SEGURIDAD INFORMÁTICA EN EL SISTEMA OPERATIVO LINUX EN SUS DIVERSAS DISTRIBUCIONES APLICADAS A LAS TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE GRADO COMO REQUISITO PARA OPTAR AL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

YEIMAR ALONSO CASTRO MATURANA

YENNY STELLA NÚÑEZ ÁLVAREZ
DIRECTOR DE TRABAJO DE GRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA (ECBTI)
TURBO, COLOMBIA
2021

NOTAS DE ACEPTACIÓN

_____

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

DEDICATORIA

Dedicatoria especial a mi madre que siempre me ha apoya incondicionalmente en mi vida.

AGRADECIMIENTOS

Agradezco a mi familia, tutores, compañeros y amigos que me apoyaron en el trascurso de la realización de mi especialización y de esta monografía son y serán un gran apoyo siempre.

TABLA DE CONTENIDO

Pág.

1. INTRODUCCIÓN 11
2. DEFINICIÓN DEL PROBLEMA 13
   2.1. PLANTEAMIENTO DEL PROBLEMA 13
   2.2. FORMULACIÓN DEL PROBLEMA 13
3. JUSTIFICACIÓN 14
4. OBJETIVOS 15
   4.1. OBJETIVO GENERAL 15
   4.2. OBJETIVOS ESPECÍFICOS 15
5. MARCO DE REFERENCIAL 16
   5.1. MARCO TEÓRICO 16
      5.1.1. Breve reseña de Linux 17
   5.2. MARCO CONCEPTUAL 18
   Sistema operativo 18
      5.2.1. Código abierto 19
      5.2.2. Sistemas operativos para servidores 19
      5.2.3. Sistemas operativos derivadas del Core de Unix 19
      5.2.4. Contraste de las distribuciones del sistema operativo Linux 19
   5.3. MARCO LEGAL Y NORMATIVIDAD 21
      5.3.1. La Licencia Pública General de GNU (GNU-GPL) 21
6. LINUX UNA ALTERNATIVA VIABLE Y CONFIABLE 24
   6.1. SEGURIDAD EN LINUX 24
      6.1.1. Características de seguridad de Linux 25

6.1.2. Ventajas y Desventajas 26
6.1.3. Versiones o/y Distribuciones Linux orientadas a la seguridad informática 26
6.1.4. Distribuciones diseñadas como muros de fuegos y UTM 31
6.1.5. Distribuciones para Pentesting, Análisis Forense y Auditorías 33
6.1.6. Distribuciones de Linux enfocadas a empresas y servidores 36
6.2. CentOS 39
6.2.2. Distribuciones de Linux enfocadas a smartphones 44
6.2.3. Porción del mercado en servidores Linux 47
6.2.1. Distribuciones Linux orientadas a la programación 47
6.2.2. Distribuciones de Linux más usadas en laptops 49
7. VULNERABILIDADES Y AMENAZAS EN DISTRIBUCIONES LINUX 51
7.1. ESCALAMIENTO DE PRIVILEGIOS EN FREEBSD 51
7.2. CVE-2014-3153 Detección de TowelRoot y exploits 51
7.3. EREBUS 52
8. . HERRAMIENTAS Y BENEFICIOS DE LAS DISTRIBUCIONES LINUX 54
8.1. CLAMAV 54
8.2. WIRESHARK 55
8.3. NMAP 57
8.4. OSQUERY 58
8.5. METASPLOIT FRAMEWORK 58
9. CONCLUSIONES 60
10. RESULTADOS 61
11. RECOMENDACIONES 62
12. BIBLIOGRAFÍA 63

LISTA DE FIGURAS

Pág.
Figura 1 Kali Linux 27
Figura 2 Vista del proyecto Openwall de Linux 29
Figura 3 Subgrph OS 30
Figura 4 Distribución Clear OS 32
Figura 5 Interfaz Openwall 33
Figura 6 Distribución BackBox Linux 34
Figura 7 Estadísticas de Dispositivos que usan Santoku Linux 35
Figura 8 Distribución red hat de Linux 36
Figura 9 Linux SuSe 40
Figura 10 Ubuntu server 42
Figura 11 S.O Android 46
Figura 12 Porción del mercado respecto a otros Sistemas Operativos para servidores. 47
Figura 13 Distribuciones que más se usan es laptops 50
Figura 14 Ataque Ransomware Erebus 53
Figura 15 Entorno grafico ClamAV 55
Figura 16 Herramienta WireShark en Kali Linux 56
Figura 17 Herramienta Nmap en Kali Linux 57
Figura 18 Herramienta Metasploit en Kali Linux 59

RESUMEN

Linux es sistema un sistema operativo igual como sus homólogos Windows y Macintosh pero con la gran diferencia de ser usado de forma no lucrativa como lo hacen otras contrapartes que sacan rentabilidad por el uso de sus servicios es sus diferentes versiones y funcionalidades. Linux es y ha sido alimentado por una comunidad a través del mundo entero con sus aportes a las diversas distribuciones que lo abastecen día a día. Linux nace como un entretenimiento por entonces joven llamado Linux Torvalds por aquel entonces cursado su vida universitaria en el campus de la universidad de Helsinki en Finlandia. A través de los años el sistema operativo Linux ha ganado adeptos y una gran comunidad que lo avala y lo autoriza a tener una porción del mercado de los sistemas operativos bastante sustancias con sus diversas distribuciones que cumplen múltiples propósitos para los usuarios emparentados y simpatizados con Linux por su funcionalidades prestadas en sus distribuciones; funciones que van desde ofrecer seguridad como lo es Red Hat y Debian, integridad como lo es Ubuntu, distribución y manejo de recursos como CentOS, protección en la de como Open SuSE y hasta proyectos de vulnerabilidades como Kali Linux anteriormente llamada Backtrack.

Teniendo en cuenta el contexto de lo que es Linux esta monografía busca exponer las bondades de las diferentes distribuciones de Linux para la seguridad informática para los usuarios finales, organizaciones, empresas y comunidad que hace uso de Linux como sistemas operativos. En esta monografía argumentare aspectos positivos y relevantes del sistema operativo Linux que permitirán tener en cuenta su usabilidad, disponibilidad, integridad y seguridad en los diferentes dispositivos, medios y herramientas que constituyen un sistema gestor de información. Esta monografía no busca explicar el uso del sistema operativo Linux para el hacking ético esta monografía pretende exponer como las diferentes distribuciones de Linux aportan a la seguridad informática desde la perspectiva del usuario final o el usuario común.

Palabras Clave: Seguridad informática, Sistemas Operativos, Linux, Amenazas, Riesgo, Servidores, Computadoras, Distribuciones.

ABSTRACT

Linux is an operating system the same as its Windows and Macintosh counterparts but with the great difference of being used in a non-profit way as other counterparts do that get profitable for the use of their services in their different versions and functionalities. Linux is and has been fed by a community throughout the world with their contributions to the various distributions that supply it day by day. Linux was born as a then young entertainment called Linux Torvalds at that time he studied his university life on the campus of the University of Helsinki in Finland. Over the years, the Linux operating system has gained adherents and a large community that endorses it and authorizes it to have a fairly substantial portion of the operating system market with its various distributions that serve multiple purposes for users related to and sympathetic to Linux. for its functionalities provided in its distributions; functions that range from offering security such as Red Hat and Debian, integrity such as Ubuntu, distribution and management of resources such as CentOS, protection in how to Open SuSE and even vulnerability projects such as Kali Linux previously called Backtrack.

Taking into account the context of what Linux is this monograph seeks to expose the benefits of the different distributions of Linux for computer security for end users, organizations, companies and community that makes use of Linux as operating systems. In this monograph I will argue positive and relevant aspects of the Linux operating system that will allow us to take into account its usability, availability, integrity and security in the different devices, media and tools that constitute an information management system. This monograph does not seek to explain the use of the Linux operating system for ethical hacking. This monograph aims to expose how the different distributions of Linux contribute to computer security from the perspective of the end user or the common user.

Keywords: Computer security, Operating Systems, Linux, Threats, Risk, Servers, Computers, Distributions.

1. INTRODUCCIÓN

Los sistemas operativos forman parte fundamental de la administración, procesamiento y gestión de los procesos de la información tanto personal como organizacional teniendo un valor preponderante la seguridad informática, debido los sistemas operativos se han convertido en parte imprescindible a tal punto de formar parte de las fases más esenciales de las nuestras vidas.

Son muchas las alternativas de sistemas operativos que han surgido en la historia empresas como Microsoft con su primer sistema operativo llamado MS-DOS actualmente llamado Windows, encontramos a Apple con su sistema operativos Macintosh que surgió como una forma revolucionaria y segura de gestionar la información de los usuarios que adoptaran su sistema operativo en sus máquinas.

Los sistemas operativos anteriores a pesar de contar con una popularidad son costosos comercialmente por su naturaleza copyright (licencias de compra) y consumir sus recursos requieren de un capital para obtenerlos y para inicio de la era de los 90's nace una alternativa la cual permitía usar libremente las características de los 2 sistemas operativos anteriores curiosamente usando el mismo kernel (núcleo) llamado **Unix** en los cuales los demás sistemas operativos usar para basar sus sistemas operativos. Es así como en los años noventa surge Linux una alternativa de uso gratuito (Free) por parte de Linus Trovals con muchos de los componentes de los sistemas operativos del mercado, pero en este caso gratis y avalado por una comunidad Free Software Foundation.

El sistema operativo Linux cuenta con su código fuente de forma libre y gratuita soportado por la comunidad su uso y modificación por parte de terceros es avalado y no tiene ningún conflicto legal con sus fundadores y comunidad y debido a esta característica el sistema operativo Linux es flexible en diversos contexto con tanto con distribuciones que se especializan en sectores como la seguridad informática, administración de recursos específicamente hardware y software, repositorios y demás dependencias.

Sus distribuciones se han convertido en sinónimo de seguridad en la comunidad mundial desde sus primeras versiones como lo son Debian, SuSE y Mandrake hasta sus versiones actualizadas como Red Hat, Fedora y Ubuntu. Y aunque su uso durante años fue resistido por su naturaleza o por sus interfaces controvertidas Linux hoy en día tiene un lugar y porción de mercado creciente y que confía en sus características como de disponibilidad, integridad, recursividad, multiplataforma, pero sobre todo su seguridad.

Linux a través de sus diversos proyectos sigue creciendo como un estandarte de la seguridad informática desde el usuario final hasta las corporaciones y organizaciones que hacen uso de Linux como su principal sistema operativo para ser más precisos hablamos de casos como IBM, Intel, Lenovo, ADM, Google, Dell,

Asus y demás colosos de las tecnologías que confían su información y seguridad a un sistema operativos totalmente gratuito y de uso libre.

2. DEFINICIÓN DEL PROBLEMA

2.1. PLANTEAMIENTO DEL PROBLEMA

Los sistemas operativos son la base fundamental de los sistemas de información y por ende importante actor de la seguridad de la información de la cual es el encargado de administrar, proteger y gestionar. Dentro de sus múltiples actividades y funciones los sistemas operativos se encargan esencialmente de la comunicación del hardware (toda la parte física) con el software (la parte lógica) siendo un excelente interprete de ambas partes con su kernel por ende los sistemas operativos deben contar con diversos niveles de seguridad para llevar a cabo esa función de mediador, comunicador y traductor de todo aquello que transite entre lo análogo y lo digital.

En el caso particular Linux es uno de los sistemas operativos más comunes y populares en el mundo debido a su filosofía Opensource, su adquisición es de forma gratuita y no posee ningún costo comercial a diferencia de sus homólogos Windows y MacOS surge como la alternativa más opcional para satisfacer las necesidades de seguridad informática por la naturaleza de las virtudes anteriormente mencionadas. A lo que me hace preguntar ¿qué tan seguro es el sistema operativos Linux a pesar de ser gratuito? O ¿Qué tan vulnerable puede llegar a ser Linux?, ¿Qué lo hace tan confiable?, ¿Cuenta con característica de seguridad necesaria para su uso comercial?, ¿Es soportado por una comunidad que avala su uso?, ¿Existen organizaciones o corporaciones que lo usen como su sistema operativo de pila o predeterminado? son muchos interrogantes lo cual nos lleva a una problemática generalizada de la seguridad prestada por Linux como sistema Operativo.

2.2. FORMULACIÓN DEL PROBLEMA

¿Es viable y seguro el uso del sistema operativo Linux como herramienta de seguridad informática en entornos comerciales, corporativos, organizacionales y personales para mitigar, prever o proteger la información y recursos que este bajo su custodia a diferencia de sus rivales comerciales que cuenta con herramientas con una reputación y figura de copyright?

3. JUSTIFICACIÓN

Un gran porcentaje de empresas, compañías y empresas están empezando a usar a Linux como proveedor de sistemas de operativos por sus políticas Opensource y sus diversas distribuciones dedicadas a servicios particulares dependiendo la distribución que se necesite Debían, SuSE, Ubuntu, Fedora, Mandria entre otras distribuciones lo que se constituye como confianza y fiabilidad en la seguridad que brinda el sistema operativo Linux en las compañías del mercado actual casos puntuales de éxitos podemos mencionar a GitHub, Amazon que usa Red Hat, Google que usa una distribución basa en Linux llamada Goobuntu y hasta la misma NASA. Linux brinda unas múltiples gamas de posibilidades en el momento de interactuar con servidores, ofreciendo a sus interesados una plataforma flexible y de cómodo acceso.

Esta monografía afronta este tópico desde una visión completamente hipotética dándole una alternativa de conocer el sistema operativo Linux y sus distribuciones desde un punto de vista enfocado a su variedad y capacidad y no como una elección comercial.

Esta monografía tiene como finalidad brinda un mayor conocimiento de las diversas distribuciones de Linux que pueden cubrir diferentes aspectos y ámbitos de la seguridad informática tales como infraestructura, información, datos y muchos más.

Para cumplir con todo lo anteriormente mencionado se pretende detallar el uso, características, requerimientos técnicos, ventajas y desventajas de las diferentes distribuciones de Linux y el ámbito al que pertenecen como, por ejemplo: Servidores, firewall, smartphone, auditoria, informes forenses, usuarios finales y entre otros.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Ofrecer una alternativa en forma de monografía que exponga la importancia del uso y la implementación del sistema operativo Linux con sus diversas distribuciones como plataforma que brinda todos los aspectos relevantes de la seguridad informática en equipos de cómputos, servidores, redes y usuarios finales que tengan como primicia y prioridad el uso de Linux como sistema operativo principal.

4.2. OBJETIVOS ESPECÍFICOS

- Indagar acerca del Software Libre LINUX como Sistema Operativo para mostrar y denotarlo como una alternativa al uso de software de tipo rigth, de pago o comercial.
- Definir las principales distribuciones o núcleos de Linux especializadas en hábitos de seguridad informática tales como Ubuntu, Opensuse, Redhat, Debian entre otras.
- Identificar las características más relevantes de las principales o líneas básicas de las distribuciones de sistema operativo Linux tales como Ubuntu, Debian, Opensuse, Redhat entre otra y su software uso libre.
- Identificar las vulnerabilidades, amenazas que afectas las distribuciones de Linux base, así como las posibilidades de soporte, para cada uno de los tipos de usuarios, para contar con un punto de vista determinante en el momento de realizar una elección apropiada.

5. MARCO DE REFERENCIAL

5.1. MARCO TEÓRICO

Hardening o **endurecimiento** es el procedimiento por el cual asegurar un sistema de resguardarse de ataques o vacíos de seguridad. Es el método de interceptar los medios para los ataques más comunes. Consiste en el frecuente cambio de contraseñas y claves por defecto, desinstalar el software y descartar usuarios y accesos redundantes; también descalificar servicios que en desuso y robustecer las configuraciones de aquellos que estarán en uso[1].

Seguridad Informática: es la ciencia de la seguridad de la información que pretende resguardar los datos que usada por una subestructura tecnológica e informática o de comunicaciones tecnológicas para ser recolectada o comunicada. Para ello distinguiremos los siguientes tipos de seguridad:

Seguridad física: se relaciona con la protección del material físico del sistema ya sea medios magnéticos e infraestructuras ante ataques, agresiones, amenazas, inundaciones, conflagraciones, hurtos, etc.

Seguridad lógica: pretende proteger la parte intangible de un sistema informático (programas, información, datos y sistemas operativos). Una de las ciencias usadas es la criptografía[2].

• **Seguridad activa**: es la delegada de advertir, descubrir e impedir cualquier evento no deseado en los sistemas informáticos previo de que se genere (medidas provisorias). Por ejemplo, uso de contraseñas[3].

---

[1]Hardening. [Sitio web]. [Fecha de consulta 7 febrero 2021] disponible en : https://hardeningpatching.weebly.com/hardening.html

[2] Arquiñano, c. [Sitio web]. Seguridad Informática Mc Graw-Hill [Sitio web]. [Fecha de consulta 7 febrero 2021] disponible en : https://www.academia.edu/8358689/Seguridad_Informatica_Mc_Graw_Hill_2013_www_Free_Libros_me_copia

[3] Arquiñano, c. [Sitio web]. Seguridad Informática Mc Graw-Hill [Sitio web]. [Fecha de consulta 7 febrero 2021] disponible en : https://www.academia.edu/8358689/Seguridad_Informatica_Mc_Graw_Hill_2013_www_Free_Libros_me_copia

• **Seguridad pasiva**: alcanza aquellos métodos o maneras necesarias para reducir los efectos de una peripecia de seguridad (forma correctiva). Tales como: las copias de seguridad, puntos de restauración y otras[4].

5.1.1. Breve reseña de Linux

A principios de los años 80's Richard Stallman creó desarrollo el proyecto lo que hoy se conoce como **GNU**, con la firme intención de erigir sistemas similares a UNIX y que a su vez interactuaran con POSIX. En los posteriores años creo "Fundación del Software Libre" y trazó la guía general de licencias públicas para facilitar el uso software libre en un mundo gobernado por el copyright[5].

A medida que el software libre se expandía de manera muy rápida y exponencial principios de los años 90's existía tanto software libre y de código abierto como para crear un sistema operativo sus propias manos pero faltaba una parte necesariamente importante un núcleo o un kernel para materializar dicha propuesta.

El sistema operativo Linux surge a inicios de los años 90's como una iniciativa del estudiante de la de informática de la Universidad de Helsinki en Finlandia llamado Linus Torvalds su idea era realizar un sistema operativo que fuera compatible con el sistema operativo Unix. Inicialmente las distribuciones de Linux no contaban con los nombres que conocemos hoy en día, la primera versión no comercial del sistema operativo Linux se conoció como Linux 0.0.1 basada en lenguaje c (assembler), luego se lanza la versión 0.0.2 que ya contaba con un compilador de GNU a C dándole actualmente el nombre de GNU/Linux[6].

Las más famosas se hallan **Mandriva, Manjaro, Fedora, Debian, Ubuntu** y muchas otras, que a su vez pueden ser refactorizadas o mejoradas por el usuario final o experto de acuerdo con sus prioridades, lo que da como resultado el surgimiento de otras nuevas versiones fundamentadas en versiones anteriores.

---

[4] Arquiñano, c. [Sitio web]. Seguridad Informática Mc Graw-Hill [Sitio web]. [Fecha de consulta 7 febrero 2021] disponible en : https://www.academia.edu/8358689/Seguridad_Informatica_Mc_Graw_Hill_2013_www_Free_Libros_me_copia

[5] José Romero, C. [Sitio web]. Sistema Operativo LINUX. [Fecha de consulta 7 febrero 2021] disponible en https://sistemaoperativolinuxune.blogspot.com/

[6] Miranda, J. [Sitio web]. Breve historia de Linux. . [Fecha de consulta 7 febrero 2021] disponible en http://www.iuma.ulpgc.es/users/jmiranda/docencia/libro_ada/libro_ada_html/node133.htm

5.2. MARCO CONCEPTUAL

Seguridad Informática: radica en preservar los recursos de un sistema de información (principalmente software) de una estructura organizacional sean usados de la manera más correcta posible y que su disponibilidad y acceso a dicha información allí resguardad, como su manipulación, sólo sea posible acreditado personal encargado y dentro de los términos de su autorización"[7]. Otra definición de seguridad informática también es una rama que se deriva y procura de proteger la información que usada una subestructura informática y de comunicaciones para ser recopilada o transferida[8].

Sistema operativo

"Un sistema informático, es un conjunto de elementos relacionados entre sí que tiene como finalidad el apoyar al usuario en el desarrollo de soluciones, para entender mejor esto puede dividirse en cuatro componentes básicos: el hardware, el Sistema Operativo, los programas de aplicación y los usuarios. El hardware (Unidad Central de Procesamiento (UCP), memoria y dispositivos de entrada/salida (E/S)) proporciona los recursos de computación básicos. Los programas de aplicación (compiladores, sistemas de bases de datos, juegos de video y programas para negocios) definen la forma en que estos recursos se emplean para resolver los problemas de computación de los usuarios".[9]

"Un sistema operativo es un programa de sistema que se encarga de administrar los recursos con que cuenta una computadora. Los recursos se dividen en:

- Recursos de hardware, por ejemplo, el teclado, el ratón, la impresora, etc.

- Recursos de software, por ejemplo, el compilador de un lenguaje de programación, un procesador de texto, etc." Hernández, Pérez, Flor Ángel. Sistema operativo Windows: presente y futuro.[10] (Hernández)

---

[7] Albornoz, L. [Sitio web]. El riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas BASC. [Fecha de consulta 7 febrero 2021] disponible en: https://www.academia.edu/28646328/El_riesgo_y_la_falta_de_pol%C3%ADticas_de_seguridad_inform%C3%A1tica_una_amenaza_en_las_empresas_certificadas_BASC

[8] Escrivá, G. G. Seguridad informática. Macmillan Iberia, S.A. 2013

[9] SISTEMAS, A. [Sitio web]. Auditoria de sistemas. [Fecha de consulta 7 febrero 2021] disponible en: https://portafolioauditoriasistemas.blogspot.com/2009/04/

[10] Pérez Hernández, M., & Duarte, A. *La informática, presente y futuro en la sociedad* .Córdoba: El Cid Editor. 2006. p.1

5.2.1. Código abierto

“Es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de poder acceder al código, que a las cuestiones éticas y morales las cuales se destacan en el software libre.”

“En muchas ocasiones se confunde el concepto de software libre con el de software gratuito (en inglés, free tiene los dos significados), en posteriores documentos se aclaró que el software libre no tiene por qué ser gratuito. Hay entender como software libre programas de los que podemos conseguir su código fuente, estudiarlo, modificarlo y redistribuirlo sin que nos obliguen a pagar por ello”. Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest E-book [11]

5.2.2. Sistemas operativos para servidores

“En el mercado existen diversos sistemas operativos especializados para funcionar como servidores, los más utilizados son los de las familias de Microsoft Windows o alguna distribución de Linux”[12].

5.2.3. Sistemas operativos derivadas del Core de Unix

Linux como sistema operativo dentro de su haber posee diversas distribuciones, para hacer mención de algunas y de su extenso catálogo podemos decir las siguientes en un orden no jerárquico ni cronológico: Ubuntu, Gentoo, SuSE, Debian, Red Hat, Mandriva, Fedora entre otras.

5.2.4. Contraste de las distribuciones del sistema operativo Linux

“Fedora es un Sistema Operativo Linux que cuenta con una amplia aceptación por parte de la industria, con lo último y lo más nuevo en software libre y de código abierto. Su versión actual a diciembre de 2009 es la versión 12”[13].

---

[11] Arena, H. *Linux avanzado*. Buenos Aires: MP Ediciones. 2000

[12] Martínez, S. [Sitio web]. Introducción a la ingeniería de sistemas. [Fecha de consulta 7 febrero 2021] disponible en: https://www.academia.edu/24927405/Introduccion_a_la_ingenieria_de_sistemas

[13] MANCILLA, J. [Sitio web]. [Fecha de consulta 7 febrero 2021] disponible en: https://juancarlosbaccamancilla.blogspot.com/

“Ubuntu Server también es una distribución Linux que va ganando adeptos como Sistema Operativo para servidores. Cuenta con una gran cantidad de repositorios de software y actualmente se encuentra en su versión 9.10”[14].

Red Hat (fundamentada en Fedora), es una distribución con amplio reconocimiento en la comunidad con un soporte constante y su robustez permite a las empresas implementar las soluciones que requieren alto rendimiento y calidad en los servicios que ofrecen un ejemplo de ellas es Openshitf con Red Hat Enterprise Linux 5.3[15].

Finalmente, una versión de Linux muy usada para servicios web y bases de datos es SuSE Linux, que cuenta con utilidades muy eficaces que facilitan la operación de paquetes, integración con tecnologías del Sistema operativo Windows.

Fedora Core es una distribución totalmente gratuita, basada Red Hat, pero a diferencia de ésta, posee una comunidad que la soporta, lo que es una gran ventaja ya que los cambios, modificaciones, actualizaciones y correcciones a fallos suelen demorar menos tiempo. Una desventaja su complicado manejo para usuarios con un nivel básico o mínimo de conocimiento en Linux.

“Ubuntu Server es otra distribución de Linux basada en Debian, completamente gratuita y que cuenta con un gran repositorio de software. Por defecto no incluye entorno gráfico, aunque es posible instalarlo y configurarlo. Este sistema operativo es soportado por la comunidad. Tiene gran aceptación a nivel mundial por su gran facilidad de uso, incluso para personas con conocimientos básicos en Linux. Es bastante rápido y se puede ejecutar en computadoras con bajos recursos. Además de ofrecer actualizaciones automáticas de manera constante”. [16]DistroWatch, noticias, enlaces, información y actualización, ranking de popularidad, Software [en línea] [bibliografía solamente

“El sistema operativo Red Hat Enterprise es una distribución de Linux de código abierto, que sin embargo no es gratuita, pero cuenta con actualizaciones continuas y un gran soporte por parte de la corporación que lo desarrolla. Es ampliamente utilizado en un sin fin de empresas medianas y grandes, ya que ofrece soluciones robustas y acordes a las necesidades de la mayoría de las empresas. Cuenta

---

[14] granja de servidores [Sitio web]. - practicaelectiva1. Fecha de consulta 7 febrero 2021]

disponible en: https://sites.google.com/site/practicaelectiva1/granja-de-servidores

[15] Mancilla, j. [Sitio web]. JUAN CARLOS BACCA MANCILLA. [Fecha de consulta 7 febrero 2021] disponible en: https://juancarlosbaccamancilla.blogspot.com/

[16] DISTROWATCH [Sitio web]. noticias, enlaces, información y actualización, ranking de popularidad, Software [consulta: 14 de abril del 2020]. Disponible en: https://distrowatch.com/?language=ES

además con una integración muy buena con sistemas de las familias Windows y Unix". DistroWatch, noticias, enlaces, información y actualización, ranking de popularidad, Software

"SuSE Linux Enterprise Server es otra distribución de Linux que también es de código abierto y al igual que Red Hat Enterprise no es gratuita, pero cuenta con el soporte de Novell y con una amplia integración con sistemas operativos de Microsoft, ya que Novell y Microsoft han trabajado para ello. Esto representa una gran ventaja para las empresas que combinan ambas tecnologías, ya que hace más fácil, más rápido y menos costoso este proceso".[17]

"Mandrake Linux (antiguo nombre de Mandriva), creada por Gaël Duval, es una distribución que ha experimentado un enorme aumento de popularidad desde su primera versión de julio de 1998. Los desarrolladores partieron de la distribución de Red Hat, cambiaron el entorno de escritorio predeterminado por KDE, y añadieron un instalador fácil de usar rompiendo el mito de que Linux es difícil de instalar. Las herramientas de detección de hardware de Mandrake y sus programas para el particionamiento de discos son consideradas por muchos como las mejores de la industria, y muchos usuarios se encontraron usando Mandrake allí donde otras distribuciones no habían conseguido entregar la usabilidad necesaria. Desde entonces Mandrake Linux ha madurado y se ha convertido en una distribución popular entre los nuevos usuarios de Linux y aquellos hogares que buscan un Sistema Operativo alternativo"[18]. (Rosero, 2007)

5.3. MARCO LEGAL Y NORMATIVIDAD

5.3.1. La Licencia Pública General de GNU (GNU-GPL)

"La Licencia Pública General (más conocida por su acrónimo en inglés GPL) es con diferencia la licencia más conocida de todas las licencias del mundo del software libre. Su autoría corresponde a la Free Software Foundation y es también la licencia más utilizada (más del 70% de los proyectos), incluso por proyectos con tanta reputación del mundo del software libre y código de fuente abierto como Linux"[19]. ((Stella Rodríguez)

---

[17] STELLA RODRÍGUEZ, G. El software libre y sus implicaciones jurídicas [en línea] 2008 pág. 1-7 [consulta: 16 de marzo 2020] ISSN 0121-8697. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000200007

Una licencia GPL procura certificar la autonomía de participar y transformar software libre más allá del ámbito contractual, certificando que el software sea gratuito y libre para todos usuarios que hagan uso de GPL.

"La licencia de Linux no cuesta nada y fue creada para garantizar que esto siga siendo así. Antes del proyecto GNU, los programadores que querían distribuir gratuitamente sus programas los ponían bajo el dominio público. El problema que originaba esto, es que empresas comerciales podían tomar el programa y, modificándolo un poco, ponerle licencia comercial. Esto ocurrió muchas veces. Un ejemplo de ello fue el primer navegador de páginas Web para Internet estaba en el dominio público (Mosaic). Como no existían restricciones de copyright, una Navigator. Empresa comercial tomo el software, le añadió algunas características y lo volvió un producto comercial, creando Netscape"[20].

Tipificación de las licencias:

Comercial: "Debe ser comprado, no puede ser distribuido, y solamente está disponible como código binario para los usuarios finales. Un ejemplo de este software es Microsoft Office"[21]. Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest Ebook Central.

Software de Evaluación: "Son versiones con características limitadas de software comercial, que pueden ser distribuidas libremente y que intentan ser propaganda para el software comercial". Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest Ebook Central.

Uso no Comercial: "individuos e Es software que instituciones educativas. Es licencia. Ejemplos son StarOffice y Netscape. Se puede usar Las corporaciones gratuitamente deben por comprar". Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest Ebook Central[22].

Shareware: "Son versiones completas y de libre distribución, pero tienen una licencia que obliga a ser pagada para un uso prolongado del software. Ejemplos de esto son WinZip y WinAmp"[23]. Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest Ebook Central.

---

[20] *ARENA, H. Facundo* , Linux *Avanzado: Guia del Administrador*. Buenos Aires: MP Ediciones. 2000

[21] *Ibid,*

[22] *Ibid,*

[23] *Ibid,*

Freeware: “Consisten en software que puede ser libremente usado y distribuido, pero está disponible solamente en forma binaria. Ejemplos de esto son Internet Explorer y Netmeeting”[24]. Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest Ebook Central.

Software de Fuentes Abiertas, estilo BSD: “Un grupo cerrado de individuos crea el software, Aunque y los permite la libre distribución de los binarios usuarios pueden modificar el código, generalmente no usa las modificaciones de los usuarios. El y del código fuente. Grupo de desarrollo”[25]. Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest E-book Central.

Software de Fuentes Abiertas, estilo Apache: “Es como el BSD, pero el grupo de desarrollo puede usar las modificaciones de los usuarios si son útiles. Software de Fuentes Abiertas, estilo GNU GPL: Además de las características del estilo Apache, la licencia GPL (General Public License) requiere que todos los trabajos derivados del software deben estar también bajo esta licencia. Esta característica adicional, ideada por Stallman, es la que protege al software GNU de las empresas comerciales”. Linux avanzado (2a. ed.), Editorial ICB, 2015. ProQuest E-book Central.

“El mundo del software libre no está citado en ninguna legislación. El autor ha visto la perplejidad, cuando no el regocijo con que expertos en derecho le contestaban respecto a las consultas acerca de legislación sobre el software libre. Tras la lectura de la GPL, lo más aproximado que se ha encontrado sobre legislación aplicable es el concepto mercantil de franquicia”[26]. (Martínez, 1999)

“La similitud, es bastante plausible: existe una marca comercial (nombre del programa) un propietario (el creador o dueño del copyright) que establece unos derechos de uso y explotación de la marca comercial (la licencia GPL). Existen diferencias, por supuesto, especialmente en cuanto al uso del derecho de explotación por parte de terceras personas (redistribución). En cualquier caso, se hace patente una necesidad fundamental en el software libre: el garantizar la titularidad del producto. Porque la única garantía legal aplicable en el software libre es la de la titularidad: es fundamental, para que el modelo de software libre en la empresa sea viable, que dicha titularidad sea reconocida y mantenida bajo cualquier

[24] *Ibid,*

[25] *Ibid,*

circunstancia imaginable. El programa debe estar registrado convenientemente, y la licencia de uso debe reflejar claramente este hecho"[27].

Actualmente no existe en Colombia el ambiente político apropiado para el desarrollo de un marco legal que sustente y promocione el uso del Software Libre en los diferentes niveles estatales y en la empresa privada. Quizá esto se explica básicamente porque los proponentes de las leyes en el Congreso de la República asocian equivocadamente software libre con ataques al concepto de propiedad.

6. LINUX UNA ALTERNATIVA VIABLE Y CONFIABLE

En el presente capitulo presentaremos abordaremos y explicaremos porque el sistema operativo Linux es una alternativa factible de usar para ello destacaremos como sus principales distribuciones, características ventajas y desventajas, aspectos de seguridad informática para ello contaremos con los siguientes párrafos y enunciados.

6.1. SEGURIDAD EN LINUX

Para hablar de la seguridad informática podemos hablar de 3 diferentes de seguridad informática la primera es la seguridad hardware la cual se encarga de los dispositivos físicos (equipos de cómputo, firewall, servidores proxy entre otros). La segunda es la seguridad en la red la cual se encarga de la accesibilidad a través del internet y todo lo que transite por ella es decir documentos, imágenes, datos y entre otros). Finalmente encontramos la tercera que es la seguridad software que es la cargada es necesaria para proporcionar integridad, autenticación y disponibilidad del software que este en su disposición entre ellos aplicaciones, sistemas operativos, kernel y demás denominación.

Teniendo en cuenta lo anterior y el objetivo de esta monografía que es describir la importancia del uso sistema operativo Linux como base elemental para la seguridad informática de los dispositivos que usan dicho sistema operativo además detallare las distribuciones que se encargan de cubrir diferentes aspectos de la seguridad informática como lo son el hardware, software y la red.

Esta monografía está enfocada en el hacking ético sino en la relevancia que han tenido las distribuciones del sistema operativo Linux en la seguridad informática a

[27] MARTÍNEZ, J. A [sitio web]. La empresa ante el software libre [Consulta: 19 de marzo del 2020]. Disponible en: http://es.tldp.org/COMO-INSFLUG/COMOs/La_empresa_ante_el_software_libre/

diferencia de sus competidores del mercado explorando los diferentes beneficios de las distribuciones Linux desde su uso libre, su no comercialización y sobre todo su variedad y respaldo como software GLP.

6.1.1. Características de seguridad de Linux

Argumentando las bondades del sistema operativo Linux arrancaremos porque se le considera un sistema operativo seguro a diferencia de su competidor y masivo sistema operativos Windows arrancaremos por decir que desde la jerarquía de sus usuario y la implementación de sus permiso de usuario hay una notaría diferencia entre ambos sistemas operativos partiendo de que Linux no permite ningún tipo de archivo ejecutable y ningún tipo de registro en la maquina como lo hace su homónimo con los programas que utiliza lo que lo hace engañoso para sus usuarios.

Linux en un sistema operativo multitarea es decir que puede ejecutar varias tareas a la vez; por lo cual, lo hace mucho más eficiente, en sus diversa ramificación de distribuciones hay todo tipo: de escritorio, para la seguridad, hacking ético, programación software, servidores de red y entre otras necesidades .

Las características también se expanden a la experiencia de usuario lo cual le permite usar a placer y gusto la interfaz que el usuario desea aplicar algo que no ocurre con sus otros competidores del mercado que ya tienen prestablecidas sus GUI (Interfaz gráfica de usuario) a diferencia de Linux que ofrece diversidad de entornos de escrito, Genome 3.X, KDE, UNITY, entre otros.

Es un sistema operativo adaptable tanto a entorno como a los dispositivos hardware tales como computadoras, portátiles, servidores, teléfonos móviles, videoconsolas, que opte como tenerlo como su sistema operativo principal

Continuando con las ventajas que presenta el sistema operativo Linux con respectos a otros sistemas operativos es el uso de repositorios de sus aplicativos lo cual elimina el uso de cracks, seriales y demás forma de instalaciones alternativas a Linux, para ello Linux permite la instalación de sus aplicaciones a través de la consola o terminal conectándose a su repositorio soportado por la comunidad de Linux y actualizado. Hablando de actualización Linux posee una ventaja abismal con respecto a sus competidores debido a que sus actualizaciones son constante y la reparación de bugs y daños en el sistema operativo es mucho más rápida y corregida en el menor tiempo posible.

Lo que más se destaca del sistema operativo Linux a diferencias de sus competidores son sus distribuciones la cuales están diseñada para diversas funcionalidades entre las principales se encuentra brindar seguridad informática a sus usuarios tanto finales como empresariales, se destacan muchas distribuciones entre ella red-hat, Kali Linux, Debian y otras distribuciones.

6.1.2. Ventajas y Desventajas

6.1.2.1. Ventajas

- las versiones Linux suelen ser mucho más robustas y seguras que las del sistema operativo Windows debido a sus paquetes de actualizaciones constantes y respaldo de las comunidades Linux alrededor del mundo.
- Las distribuciones Linux son más livianas, eficaces y prácticas que las versiones de Windows y aunque Windows son mucho más holgadas por sus interfaces algunas versiones de Linux asemejan esa utilidad[28].
- Linux integra protocolos y estándares de red.
- Es código fuente abierto, posee sus propias API, aplicaciones y bibliotecas y la gran parte de estas distribuciones cuenta manuales, documentación y paginas oficiales.

6.1.2.2. Desventajas

- Muchas de sus extensiones del sistema no son compatibles con otros sistemas operativos que operan en el mercado.
- Es difícil la instalación: debido a que instalación en algunas distribuciones se da por medio “Terminales” para la instalación de paquetes.
- Documentación difícil de comprender y conocimientos es muy técnicos.
- Linux no cuenta el soporte técnico como Windows debido a que lo soporta una comunidad anónima.

6.1.3. Versiones o/y Distribuciones Linux orientadas a la seguridad informática

6.1.3.1. Kali Linux

.

La primera distribución de sistema operativo Linux con la que quisiera empezar es con **Kali Linux**, esta distribución es una de las más conocida en el aspecto de la seguridad informática está basada en **Debian**. Kali Linux tiene una variedad de más de 600 de herramientas relacionada con la seguridad informática para enumerar algunas de ellas empezamos con **nmap** que permite hacer un escaneo de los puertos habilitados y por lo cual podemos observar el tránsito de la máquina,

[28] JULIÁ [sitio web]. Gadae [consulta: 17 de septiembre 2019]. Disponible en :http://www.gadae.com/blog/ventajas-utilizar-linux/

encontramos la herramienta **wireshark** que es un analizador de protocolos en red en tiempo real, la suite Aircrack-ng (programa para testeo de redes inalámbricas) y su proyecto **Metasploit** el cual permite explorar las vulnerabilidades del sistema operativo de forma muy educativa.

Figura 1 Kali Linux

Fuente: Linuxadictos, Kali Linux ya disponible en la tienda oficial de Windows 10, [sitio web]. [Consulta: 15 noviembre de 2020], disponible en: https://www.linuxadictos.com/kali-linux-ya-disponible-en-la-tienda-oficial-de-windows-10.html

Requerimientos técnicos para usar Kali Linux

"La instalación requiere al menos 10 GB de espacio en el disco duro y se recomienda al menos 1.024 MB de RAM, aunque Kali Linux puede ejecutar más de 512 MB de RAM. Instalar Kali Linux en el disco duro es mejor en cuanto al rendimiento, pero tiene el inconveniente de dedicarle todo el espacio del disco duro o particionar el disco duro y usar una partición para instalarlo, mientras que la instalación en una máquina virtual nos proporciona un sistema ligeramente más lento, pero también mucha más flexibilidad y no tenemos que modificar la configuración del disco duro"[29].

Ámbitos de uso de la distribución Kali Linux

- Detección de vulnerabilidades en las Redes de datos.
- Pruebas esenciales de penetración inalámbrica.
- Prueba de penetración web.
- Escaneo de red.
- Ingeniería social.

[29] Alamanni, M. Kali Linux Wireless Penetration Testing Essentials. BIRMINGHAM, REINO UNIDO: Packt, 2015. Pag 55-61 ISBN 9781119323983

Ventajas

- Múltiples herramientas para pruebas de penetración.
- Git – Como repositorio de codigo.
- Amplio apoyo a dispositivos inalámbricos.
- Núcleo configurado con actualizaciones de inyección.
- Soporte ARMEL y ARMHF.

Desventajas

- No es intuitivo.
- Poca documentación.

6.1.3.2. WARLINUX Web:

Esta distribución es de modo texto está diseñada para la seguridad de redes inalámbricas. Solo funciona a través de medio magnético es decir (CD o USB) y realizara de auditorías de seguridad y evaluación de niveles de seguridad[30].

6.1.3.3. Openwall

Siguiendo con más distribuciones de Linux enfocada a la seguridad la cual es llamada **Openwall.** Openwall es un proyecto basado en una distribución Linux de seguridad mejorada que está especialmente diseñado para servidores y aplicaciones. “Como su nombre lo indica, Openwall GNU/Linux extrae el código fuente y los conceptos de diseño de numerosas fuentes, lo más importante para el proyecto es su uso del kernel de Linux y partes de la tierra de usuarios de GNU, otros incluyen los BSD, como OpenBSD para su El paquete OpenSSH y la inspiración detrás de su propia cripta basada en Blowfish para el hashing de contraseñas, compatible con la implementación de OpenBSD”[31]. (seguridad, s.f.).

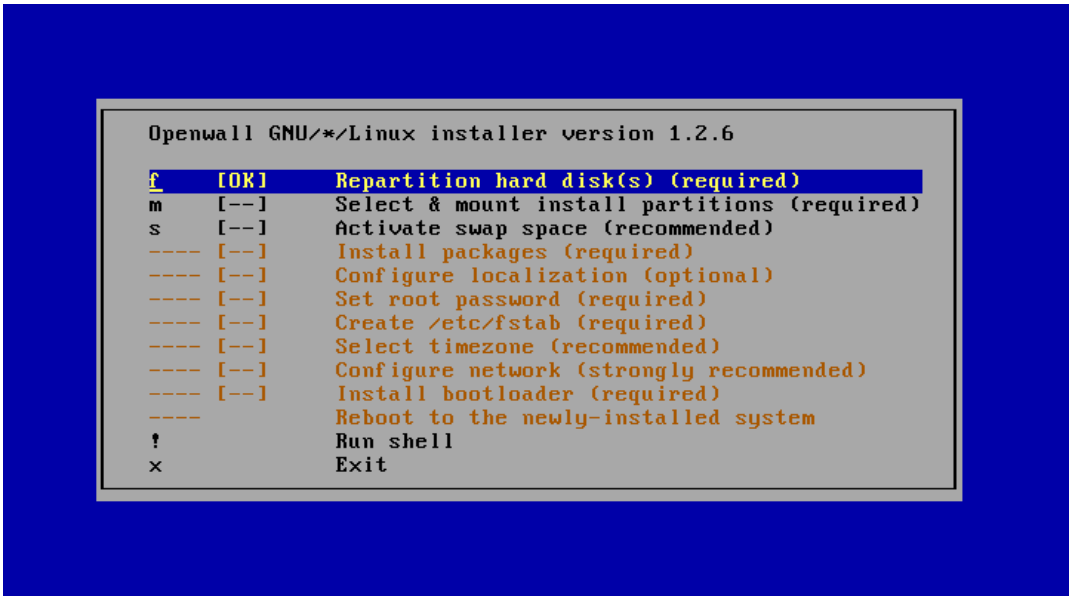
Característica de Openwall

- Acceso restringido FIFOs y enlaces en/tmp.
- Acceso restringido a/proc.
- Mejorada la aplicación del número de los procesos del usuario.
- Destrucción de segmentos de memoria compartida no está en uso.
- Otras mejoras para los núcleos pre-2.4.

---

[30] *ARENA, H. Facundo* , Linux *Avanzado: Guía del Administrador*. Buenos Aires: MP Ediciones. 2000

Figura 2 Vista del proyecto Openwall de Linux



Fuente: Openwall. Linux Kernel Runtime Guard [sitio web]. [Consulta: 13 de noviembre de 2020]. Disponible en: https://www.openwall.com/Owl/de/screenshots

6.1.3.4. Subgraph OS

No nos quedamos atrás y sigo ampliando el repertorio de distribuciones de Linux el nombre de la siguiente distribución es conocido como **Subgraph OS** esta distribución de Linux está diseñada para resistir ataques de malware y también +ataques a la red local, este nuevo sistema operativo incluye una configuración muy robusta y mitigaciones de ataques en todo el sistema operativo, gracias a que el enfoque es el de la seguridad, todas las aplicaciones que instalemos también estarán protegidas, y no solo el núcleo principal del sistema.

Esta distribución cuanta con seguridad de la memoria consiste en una herramienta desarrollada en lenguaje de programación Python las cuales son librerías basadas en el lenguaje anteriormente mencionada que impiden la corrupción de las memorias RAM que soporten el sistema Subgraph. Además, cuenta con aplicaciones firewall que detecta todo tipo de conexión. “El sistema operativo Subgraph incluye un núcleo reforzado con el muy respetado parche grsecurity / PaX para la mitigación de escalada de privilegios y explotación de todo el sistema. Además de hacer que el núcleo sea más resistente a los ataques, las características de seguridad de grsecurity y PaX ofrecen una fuerte protección de seguridad para todos los procesos que se ejecutan sin modificación (es decir, recopilación / vinculación). El kernel **Subgraph OS** también está construido con las mejoras de

seguridad RAP (demo del parche de prueba) recientemente lanzadas, diseñadas para prevenir ataques de reutilización de código (es decir, ROP) en el kernel"[32].

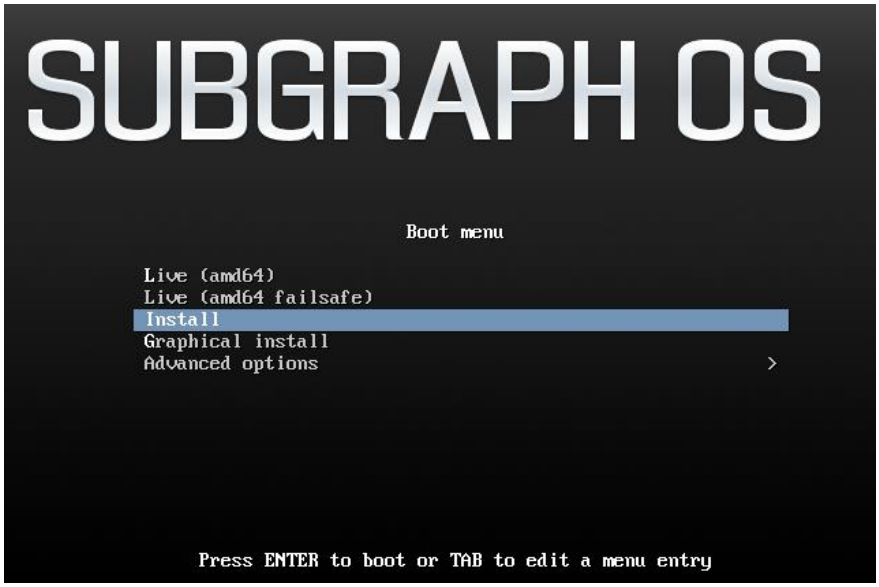
Ventajas

- Es ligera pensada en usuarios básicos.
- Opciones de configuración establecidas previamente para mejor manejo.
- invulnerable contra ataque de exploit remotos.
- Integración del navegador Tor,

Desventajas

- Limitada documentación acerca de los plugins.
- No incluye herramientas como Nmap para el escaneo de vulnerabilidades

Figura 3 Subgrph OS



Fuente: SUBGRAPH. [Sitio web]. [Subgraph OS September 2017 ISO Availability Consulta: 09 de octubre de 2020]. Disponible en: https://subgraph.com/blog/index.en.html

6.1.3.5. Whonix

"es una distribución basada en Debian GNU/Linux enfocada a la seguridad. Busca proporcionar intimidad, seguridad y anonimato en el internet. El sistema operativo consta de dos máquinas virtuales, una estación de trabajo y una pasarela a la red

[32] OS, S. [sitio web]. Subgraph OS Adversary resistant computing platform [consulta: 17 de octubre de 2019].Disponible en: https://subgraph.com/sgos/

Tor, ejecutando Debian GNU/Linux”[33]. (Greenburg, 2014). Whonix atenúa la presencia amenaza de ataques comunes generales mientras se esté usando. Mantiene anonimato on-line a través de la red Tor. Usa como base la distribución Debian altamente reconfigurada ejecutándose como una máquina virtual, proporcionando una capa sustancial de protección contra malware y fugas de direcciones IP.

6.1.4. Distribuciones diseñadas como muros de fuegos y UTM

En este ítem también encontramos distribuciones de Linux basadas en fedora, Red-Hat y Debian las cuales son interfaces para equipos que se encuentre en red convirtiéndose en una barrera protectora de los equipos con las distribuciones que mencionare a continuación.

6.1.4.1. ClearOS

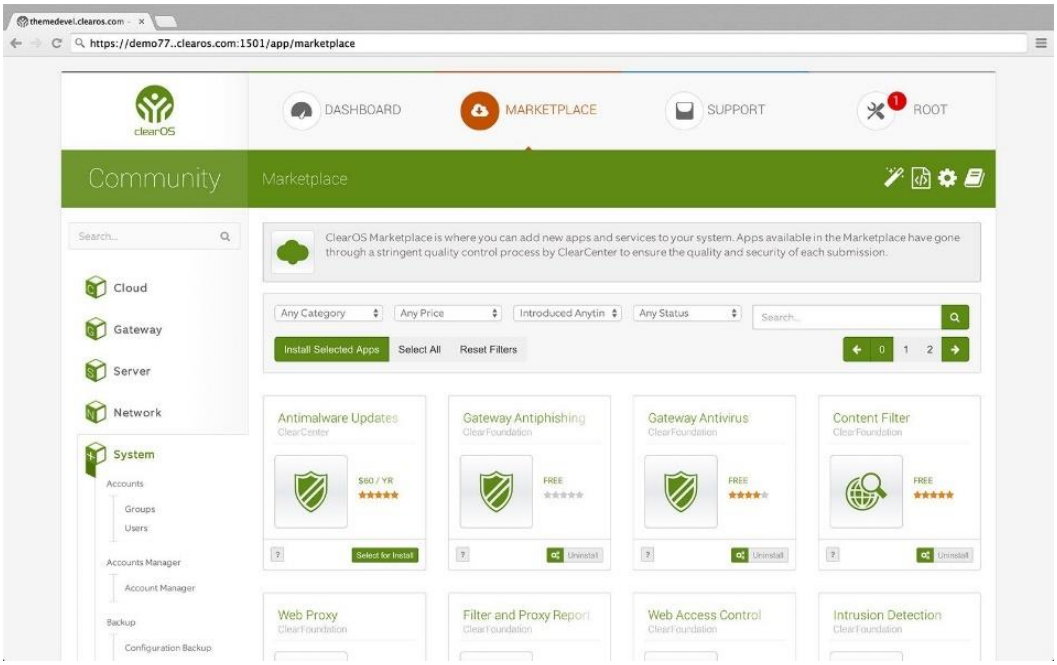
“Es un sistema operativo comercializado por la compañía de software ClearCenter. Está basado en CentOS y Red Hat Enterprise Linux, diseñado para su uso en pequeñas y medianas empresas como puerta de enlace de red y servidor de red con una interfaz de administración basada en web. Se posiciona como una alternativa a Windows Small Business Server”[34]. ClearOS. ClearFoundation. 2019-05-09.

Características principales

- Redes privadas virtuales (IPSEC y OPENVPN).
- Proxy web con filtrado de contenido y antivirus (Squid, DansGuardian).
- Cortafuegos con estado (iptables).
- Servicios de correo electrónico (Webmail, Postfix, SMTP, POP3/s, IMAP/s).

[34] ClearFoundation. [Sitio Web]. ClearSO [Fecha de consulta 7 de febrero de 2021] disponible en : https://www.clear.community/index.php/groups/55-clearfoundation

Figura 4 Distribución Clear OS



Fuente: ONWORKS. [Sitio Web]. Free Hosting Online for WorkStations. [Consulta: 23 de agosto de 2020]. Disponible en: https://www.onworks.net/distribuciones-so-es-es/basado-en-debian-es-es/clearos-gratis-en-linea-es-es

6.1.4.2. Smoothwall

"Es una distribución de Linux diseñada para ser utilizada como un firewall de código abierto.Smoothwall se configura a través de una GUI basada en web"[35] (Martin Meredith, 2019), es muy usada como un sistema firewall, aunque es carente muchas herramientas avanzadas. Es distribución flexible, ágil, no consume demasiados recursos y con interfaz web amigable.

Firewall Linux incluyen entre sus funciones principales las siguientes características:

- Firewall con reconocimiento de cambios de estados.
- Antivirus que detectan ataques provenientes de protocolos HTTP, POP3, SMTP y FTP.
- Filtro de Contenido Web.
- Antivirus Anti-Phishing y Antispam.
- Servidor DHCP.

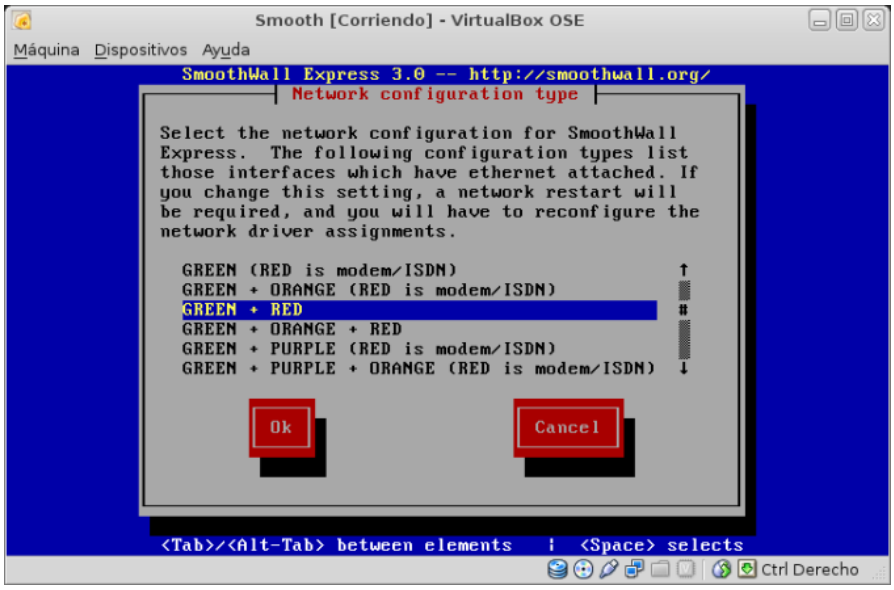
[35] MARTIN MEREDITH, N. P. [sitio web]. Techradar [consulta: 19 de septiembre del 2019]. Disponible en: https://www.techradar.com/best/best-free-linux-firewalls

- Servidor NTP.
- Sistema de detección de Intrusos.
- Soporte ADSL.
- Uso de VPN.

Desventaja

- Kernel obsoleto.
- Interfaz por agradable para su utilización.

Figura 5 Interfaz Openwall



Fuente: Openwall. [Sitio web]. Linux Kernel Runtime Guard [Consulta: 13 de noviembre de 2020]. Disponible en: https://www.openwall.com/Owl/de/screenshots

6.1.5. Distribuciones para Pentesting, Análisis Forense y Auditorías

6.1.5.1. BackBox

"Es una distribución de Linux basada en Ubuntu orientada a pruebas de penetración y evaluación de seguridad que proporciona un kit de herramientas de análisis de redes y sistemas informáticos. Incluye un conjunto completo de herramientas necesarias para la piratería ética y las pruebas de seguridad"[36]. (López J. M., 2018)

[36] LÓPEZ, JOSÉ MARÍA [sitio web]. Linux, seguridad y análisis forense digital [consulta: 25 de marzo de 2020]. Disponible en: https://hipertextual.com/2018/12/linux-seguridad-analisis-forense-digital

Dentro de las características de esta distribución de Linux son:

- Registro de vulnerabilidad
- Escalada de privilegios
- Ingeniería inversa
- Ingeniería social
- Análisis forense
- Análisis de VoIP y análisis Inalámbrico
- Más de 70 herramientas entre las cuales se encuentran Armitage, Nmap, OpenVAS, Wireshark Kismet entre otras.

Figura 6 Distribución BackBox Linux

Fuente: LinuxanduUbuntu. . [Sitio Web].BackBox 4.1 Ubuntu based Distro Released, available to download and install. [Consulta: 23 de agosto de 2020].Disponible en: http://www.linuxandubuntu.com/home/backbox-4-1-ubuntu-based-distro-released-available-to-download-and-install

Requerimientos de sistema

- 32-bit o 64-bitprocesador.
- 512 MB (RAM).
- 6 GB Espacio en disco para instalación
- Resolución de tarjeta gráfica 800×600.

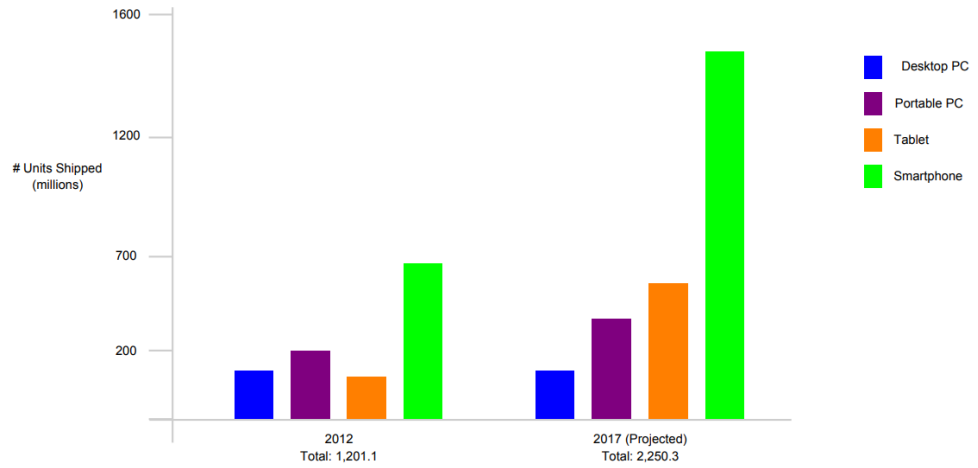
6.1.5.2. Santoku Linux

“Es una distribución basada en Linux especialmente desarrollada para auditar dispositivos móviles en busca de vulnerabilidades, fallos o simplemente cualquier aspecto que pueda comprometer la privacidad al utilizar cualquiera de estos dispositivos móviles. Disponible para los principales sistemas operativos móviles como iOS, Windows Phone, Android o BlackBerry. Este sistema operativo, que se distribuye de forma gratuita y con el código tanto del sistema como de todas las herramientas totalmente abierto y disponible para cualquiera interesado en revisarlo, incluye por defecto todos los SDK necesarios para que las herramientas funcionen sin problemas”[37].

Ventajas

- Es gratis. No requiere de ningún tipo de licenciamiento.
- Fácil de instalar y descargar por medio de LIVE CD.

Figura 7 Estadísticas de Dispositivos que usan Santoku Linux



Fuente: Archive. Mobile app análisis with Santoku Linux - Andrew Hoog. [Sitio Web].[consulta: 13 de octubre de 2020]. Disponible en: https://archive.org/details/youtube-cmVRCWbo0jU

Desventajas

- Es más difícil de utilizar y configurar que un sistema comercial.

---

[37] Ecured.cu. 2021. Santoku Linux - EcuRed. [en línea] [8 febrero 2021]. Disponible en: https://www.ecured.cu/Santoku_linux.

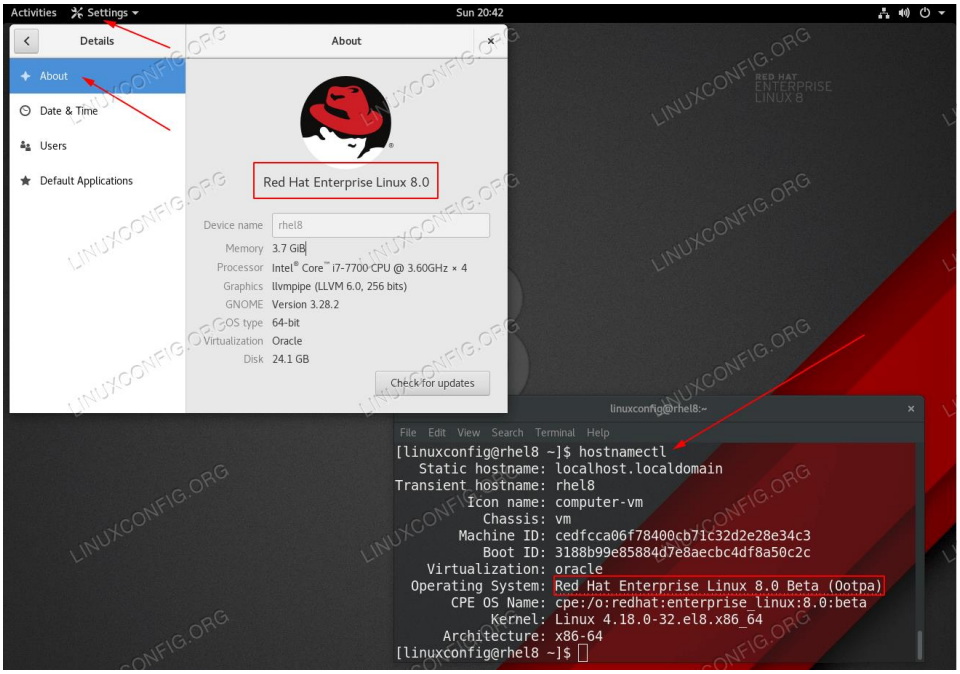
- Es menos conocido fuera del ámbito técnico por lo que su utilización puede generar inseguridad.
- Empaquetado en muchas aplicaciones legítimas, generalmente dirigidas al mercado clandestinos.
- También puede volver a empaquetar las aplicaciones después de haberlas modificado.

6.1.6. Distribuciones de Linux enfocadas a empresas y servidores

6.1.6.1. Red Hat Enterprise Linux

“Centrado para servidores y administración de grandes centros de datos o supercomputadoras. Su modelo de negocio se basa en la suscripción por servicios de mantenimiento y asistencia técnica”[38].

Figura 8 Distribución red hat de Linux



[38] López, M., [en linea]. *Seis distribuciones de Linux enfocadas a empresas*. [Consultado 8 de febrero de 2021] Genbeta.com. Disponible en: https://www.genbeta.com/linux/seis-distribuciones-de-linux-enfocadas-a-empresas.

Fuente: Linuxconfig. .[Sitio web]. How to find the version of Redhat Linux installed [Consulta: 25 de septiembre de 2020]. Disponible en: https://linuxconfig.org/how-to-find-the-version-of-redhat-linux-installed

Características de Linux Red-Hat

- Seguridad multinivel todos los servicios.
- avances en IPSEC.
- Usa Canary para la protección contra ciber ataques.
- Coexistencia con IPv6.
- Integración Microsoft y Active Directory de Windows
- Acepta encriptación de datos.
- Aplicaciones de desarrollo de aplicaciones: SystemTap y Frysk.

Ventajas

- Admite arquitecturas de hardware (Todas).
- compatibilidad con las distintas versiones.
- Incorpora interfaz de uso sencilla.
- Extensa disponibilidad aplicaciones.

Desventajas

- No soporta al formato NTFS.

6.1.6.2 Linux Debian

"Es una distribución de Linux compuesta de software libre y de código abierto, desarrollado por el Proyecto apoyada por la comunidad Debian, que fue establecido por Ian Murdock el 16 de agosto de 1993. Debian La rama estable es la edición más popular para computadoras personales y servidores, y es la base de muchas otras distribuciones"[39].

[39] Debian.org. 2021. *Debian -- About Debian*. [en linea] [8 febrero 2021]. Disponible en : https://www.debian.org/intro/about

Figura 9. Debian 9 Stretch Linux 64-bit

Fuente: Linuxconfig. .[Sitio web]. How to find the version of Redhat Linux installed [Consulta: 25 de septiembre de 2020]. Disponible en: https://linuxconfig.org/how-to-find-the-version-of-redhat-linux-installed

Características de Debian

- **Es un paquete de software: "**La mayoría de los usuarios lo que desea es el software de aplicación que se base en las herramientas que los auxilien a efectuar lo que precisen hacer, desde emitir documentos, elaborar aplicaciones de acciones hasta distraerse con los diversos juegos y emplear más software. Debian aparece con más de 50000 paquetes en software precompilado y embalado con un formato incondicional para una disposición sencilla en su artefacto, un gestor de envoltorios, y otros beneficios que crean posible tramitar cientos de paquetes en millones de ordenadores de forma tan fácil como situar una sola aplicación. Todos ellos de manera gratuita[40]".
- **Es gratis[41]:** Las comunidades respaldan el uso del software libre para conseguir observar cómo funciona este. Debían prioriza software libre por lo

[40] 12 características [sitio web]. 12caracteristicas [consulta: 20 de marzo 2020].Disponible en : https://www.12caracteristicas.com/debian/

[41] Ibid.,

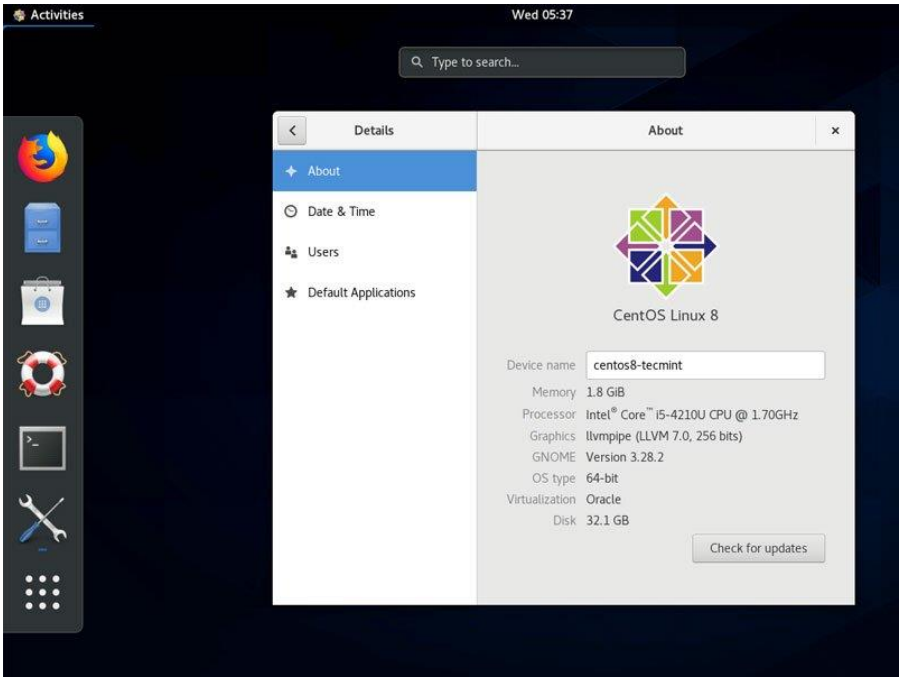
que se piensa que es útil que esa responsabilidad de formalizar en algún tipo de documento. Para lo cual nació el Contrato Social.

- **Mantiene un control[42]:** Debían manipula cualesquier paquetes situados en esa distribución, incluyendo la posibilidad de instalar un solo paquete o actualizar totalmente sistema operativo. Por lo tanto, los paquetes propios igualmente pueden protegerse de las mejoras en el repositorio.

6.2. CentOS

"es una versión de Linux que suministra una escenario libre, informática apuntalada por la agrupación funcionalmente concurrente con su algunos códigos fuente, Red Hat Enterprise Linux (RHEL) CentOS"[43].

Figura 9 CentOs



Fuente: Centos. [sitio web]. The CentOS Project . [Consulta:27 de abril de 2020].Disponible en: https://www.centos.org/

Características

---

[42] Ibid.,

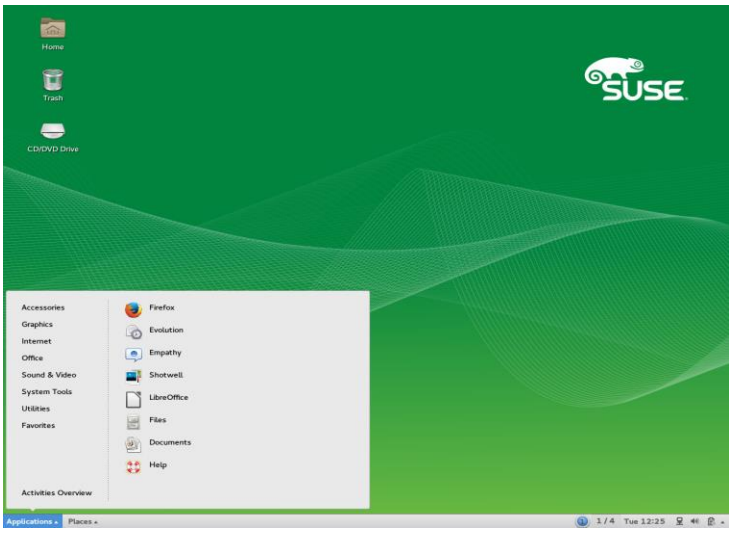
[43] CENTOS. [sitio web]. Preguntas frecuentes sobre CentOS en general. [Consulta: 12 de septiembre de 2019] disponible en: https://wiki.centos.org/FAQ/General#head-4b2dd1ea6dcc1243d6e3886dc3e5d1ebb252c194

- Una numerosa red de servidores espejos, como el IRC[44].
- Garantía de Linux Containers a través de host de control o servidor físico[45].
- XFS como sistema de ficheros con capacidad de manejar altos volúmenes de datos[46].

6.2.1.1. SUSE Linux

“usada para la gestión de servidores, virtualización de entornos y administración de centros de almacenamiento de datos”.[47]

Figura 10 Linux SuSe



Fuente: Suse.[Sitio web]. ¿Por qué SUSE?.[Consulta: 26 de septiembre de 2020]. Disponible en: https://www.suse.com/es-es/

Características técnicas:

- **Bloqueos dinámicos: “**permiten la interrupción o preferencia de secciones del kernel de Linux en las que previamente no se admitían interrupciones. La latencia se reduce al mínimo y los tiempos de respuesta son más predecibles, lo que le permite eliminar la probabilidad de que un sistema operativo no interrumpible interfiera en el proceso de alta prioridad”[48].

---

[44] Holguín, L., [en línea]. *Sistema Operativo Centos*. [Consultado: 8 Febrero 2021] Disponible en: https://luisa-holguin19.blogspot.com/2012/06/.
[45] Ibid.,
[46] Ibid.,

[47] Central, P. E [sitio web] [2015]. [Linux avanzado 2a. ed. Editorial ICB].
[48] LINUX [sitio web], S. SuSE, [consulta: 14 de abril del 2020]. Disponible en: https://www.suse.com/es-es/products/realtime/technical-information/

- **Interrupciones de ejecución de hilos de proceso: "**Las interrupciones son procesos que pueden iniciarse mediante hardware (interrupción por hardware) o software (interrupción por software) y que, una vez iniciados, hacen que el núcleo de Linux conmute del modo de proceso al de interrupción. Los procesos que se ejecutan en modo de interrupción en un sistema operativo de propósito general no disponen de preferencia. Con SUSE Linux Enterprise Real Time, estas interrupciones se hallan limitadas o encapsuladas por hilos del núcleo, que pueden interrumpirse y que permiten que los dos tipos de interrupciones mencionadas anteriormente se puedan controlar desde procesos de mayor prioridad definidos por el usuario"[49]**.**

- **Herencia de prioridades:** "Hace referencia a la capacidad de un proceso de baja prioridad para asumir una prioridad más elevada si hay un proceso de mayor prioridad que requiera la finalización del proceso de baja prioridad a fin de poder completar su tarea. Incluye una librería glibc alternativa que amplía la herencia de prioridad al espacio de usuario. Las aplicaciones que utilicen esta glibc alternativa pueden solicitar la aplicación de la herencia de prioridad a sus exclusiones mutuas POSIX"[50].

- **Protección y asignación de CPU: "**Los usuarios disponen de control absoluto sobre la asignación de procesos e hilos a los microprocesadores. Los procesos que necesiten ejecutarse en tiempo real pueden asignarse a microprocesadores o núcleos de forma exclusiva"[51].

- **Directory Server: 389** Directory Server reemplaza OpenLDAP para proporcionar un servicio de directorio sostenible.
- **Aplicaciones de servidor:** Funcionalidad básica del servidor (DHCP, DNS, Web), soporte NVDIMM, OFED.

Ventajas

- Un sistema muy estable.
- Repositorios confiables y de terceros.

---

[49] SERVER [sitio web], S. L. SUSE Linux Enterprise Server[15 abril 2019].Disponible en: https://documentation.suse.com/sles/15-SP1/

[50] SERVER [sitio web], S. L. SUSE Linux Enterprise Server[15 abril 2019].Disponible en: https://documentation.suse.com/sles/15-SP1/

[51] LINUX [sitio web], S. SuSE, [consulta: 14 de abril del 2020]. Disponible en:

https://www.suse.com/es-es/products/realtime/technical-information/

- Bajo consumo de recursos.

Desventajas:

- Algunos programas gráficos como AutoCAD no corren en Linux.

6.2.1.2. Ubuntu Server

“Es una distribución de Linux basada en la arquitectura de Debian. Actualmente corre en computadores de escritorio y servidores, en arquitecturas Intel, AMD y ARM. Está orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario. Está compuesto de múltiple software normalmente distribuido bajo una licencia libre o de código abierto”[52]. (Operating System Versión Usage (en inglés). , 2010).

Figura 11 Ubuntu server

Fuente: Linuxenespañol. [Sitio web].¿Qué es Ubuntu?. [Consulta: 23 de mayo de 2020]. Disponible en: https://www.xn--linuxenespaol-skb.com/distribuciones/ubuntu/

Requisitos mínimos recomendados

Tipo de instalación

[52] Roshy.net. Ubuntu, un OS para todos – cursos roshy. [sitio web]. [Consulta: 8 de feb. de 2021] Disponible en: http://roshy.net/sistemas/2019/03/29/ubuntu-un-os-para-todos

- **Instalador de Debian**: CPU 1 gigahertz, RAM 512 megabytes, Disco duro 1.5 gigabyte.
- **Servidor en vivo**: CPU 1 gigahertz, 1 gigabyte, RAM 1 gigabyte, Disco duro 1.5 gigabyte.
- **Instalador de Debian(mínima)**: CPU 300 megahertz, RAM 384 megabytes, Disco duro 1.5 gigabyte.

Características principales de Ubuntu Server

- **DNS server**[53]: Gestor de DNS (Domain Name Server).
- **LAMP server**[54]**:** Permute la instalación de Linux/ Apache/ MySQL o MariaDB/ PHP.
- **Servidor de correo**[55]**:** Esta opción permite que Ubuntu Server gestione los correos de la organización.
- **Servidor OpenSSH**[56]**:** Permite que la comunicación SSH sea efectiva.
- **Base de datos PostgreSQL**[57]: Permite la configuración servidores PostgreSQL.
- **Servidor Samba**[58]: Permite la transferencia de archivos entre diversos sistemas de forma segura y compatible.

Características de integralidad

- La autenticación para los equipos de una red es fundamental se registren mutuamente y consentir que la información sea distribuida. Todas las versiones de Ubuntu Server poseen la aplicación de Open LDAP que asegurar un servicio de directorio compartido si se necesario.

---

[53] Conocimiento Libre. 10 nuevas características en Ubuntu 19.04 Disco Dingo - Conocimiento Libre [Sitio web]. [Consulta: 24 de septiembre de 2019] disponible en: https://conocimientolibre.mx/ubuntu19-04-caracteristicas

[54] Ibid.,

[55] Ibid.,

[56] Ibid.,

[57] Ibid.,

[58] Ibid.,

- SAMBA: un manejador de intercambio de archivos e integrado con un Directorio Activo de Microsoft. La compatibilidad con entornos complexos es una particularidad sonada entre los usuarios de Ubuntu. Linux también es compatible con protocolos como Kerberos, SSH, NFS y muchos otros.

Características de seguridad

- "Ubuntu Server está construido sobre la gran seguridad del sistema operativo Debian. El equipo de seguridad de Ubuntu trabaja en estrecha colaboración con sus homólogos de Debian y Linux para asegurarse de que las vulnerabilidades que surgen sean reconocidas y tratadas con prontitud. El espíritu libre y justo de Ubuntu significa que los parches están disponibles para todos los usuarios, no sólo los clientes de la empresa o los abonados"[59].

Ventajas

- "La posibilidad de crear fácilmente un directorio encriptado privado de su servidor donde se puede almacenar información crítica contraseñas, nombres de usuario y conexiones".
- Se permite usar en forma privada, pública o comercial es de licencia gratuita[60].
- Es estable, liviano y es compatible.
- Fácil de usar e instalar[61].

Desventajas

- "Creará una partición swap, que es la que Ubuntu utiliza como memoria virtual"[62].
- Afecta el rendimiento, cuando es instalada en una partición en formato EXt2 o Ext3 dado que son particiones exclusivas donde se aloja Linux

6.2.2. Distribuciones de Linux enfocadas a smartphones

---

[59] BLOGSPOT. [sitio web]. Instalación, características, ventajas y desventajas del sistema operativo Linux Ubuntu server, desarrollado por canonical LTD [19 de 09 de 2019]. Disponible en: http://isft179-ubuntuserver.blogspot.com/

[60]ANTONIO, L. Ventajas & Desventajas De Linux Ubuntu [sitio web]. Obtenido de Ventajas & Desventajas De Linux Ubuntu [consulta: 22 de marzo de 2020]. Disponible en :http://loganventajasydesventajasubuntu.blogspot.com/

[61] ANTONIO, L. Ventajas & Desventajas De Linux Ubuntu [sitio web]. Obtenido de Ventajas & Desventajas De Linux Ubuntu [consulta: 22 de marzo de 2020]. Disponible en :http://loganventajasydesventajasubuntu.blogspot.com/

[62] ANTONIO, L. Ventajas & Desventajas De Linux Ubuntu [sitio web]. Obtenido de Ventajas & Desventajas De Linux Ubuntu [consulta: 22 de marzo de 2020]. Disponible en :http://loganventajasydesventajasubuntu.blogspot.com/

6.2.2.1. Firefox OS

“Es una plataforma que está basada en Linux, aunque se le han añadido las librerías pertinentes para poder controlar el hardware, poder hacer llamadas, enviar SMS. No obstante, pese a que pueda parecer que estemos ante una interfaz como la de otras plataformas móviles, Firefox OS trabaja sobre un browser (un navegador) aunque no se muestra ni barra de herramientas ni URL”[63].

6.2.2.2. Android

“el sistema Android está basado en el núcleo de Linux 3.0; las primeras versiones estaban basadas en el núcleo 2.6. Este núcleo tiene en cuenta la gestión de las capas inferiores, tales como los procesos, la gestión de la memoria, los permisos de usuario y la capa de hardware”[64]**.**

[63] ECURED [Sitio web]. Firefox OS [consulta: 14 de abril del 2020]. Disponible en https://www.ecured.cu/Firefox_OS#.C2.BFQue_es_Firefox_OS.3F

[64] Ediciones-eni.com. [sitio web]. Libro Android - Guía de desarrollo de aplicaciones Java para Smartphone y Tabletas (3ª edición). Disponible en: https://www.ediciones-eni.com/libro/android-guia-de-desarrollo-de-aplicaciones-java-para-smartphones-y-tabletas-3-edicion-9782409006104.

Figura 12 S.O Android

Fuente: Tizen. Application Developers.[Sitio web].[Consulta:05 de febrero de 2020].Disponible en: https://www.tizen.org/

6.2.2.3. Tizen

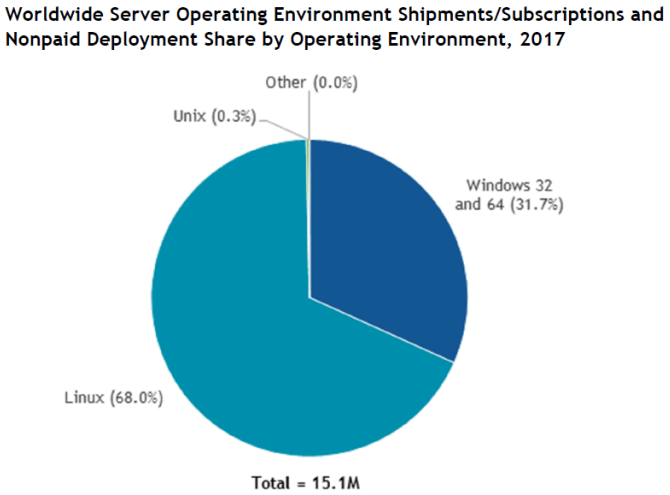
Es un sistema operativo móvil basado en Linux usado por empresa como Intel, Huawei, Fujitsu, Samsung, Panasonic, Vodafone entre otras en sus diferentes productos tecnológicos[65].

[65] Sistemas Operativos 2017-1. [sitio web], *Tizen*. [consulta:16 de marzo 2020] Disponible en: https://chsosunal20171911005.wordpress.com/2017/05/22/tizen/.

6.2.3. Porción del mercado en servidores Linux

En esta grafica representa el uso de sistemas operativos usado para entornos de servidores con sus respectivos subscriptores de los diversos sistemas operativos a nivel mundial en el año 2017.

Figura 13 Porción del mercado respecto a otros Sistemas Operativos para servidores.



Fuente: MuyLinux. Red Hat lidera el segmento Linux en el mercado de servidores. [Sitio web].[Consulta:03 de julio de 2020].Disponible en: https://www.muylinux.com/2018/10/19/red-hat-lidera-mercado-linux-servidores/

En la figura 12 se puede observar que el sistema operativo predilecto para servidores es Linux con un 68% de los encuestados.

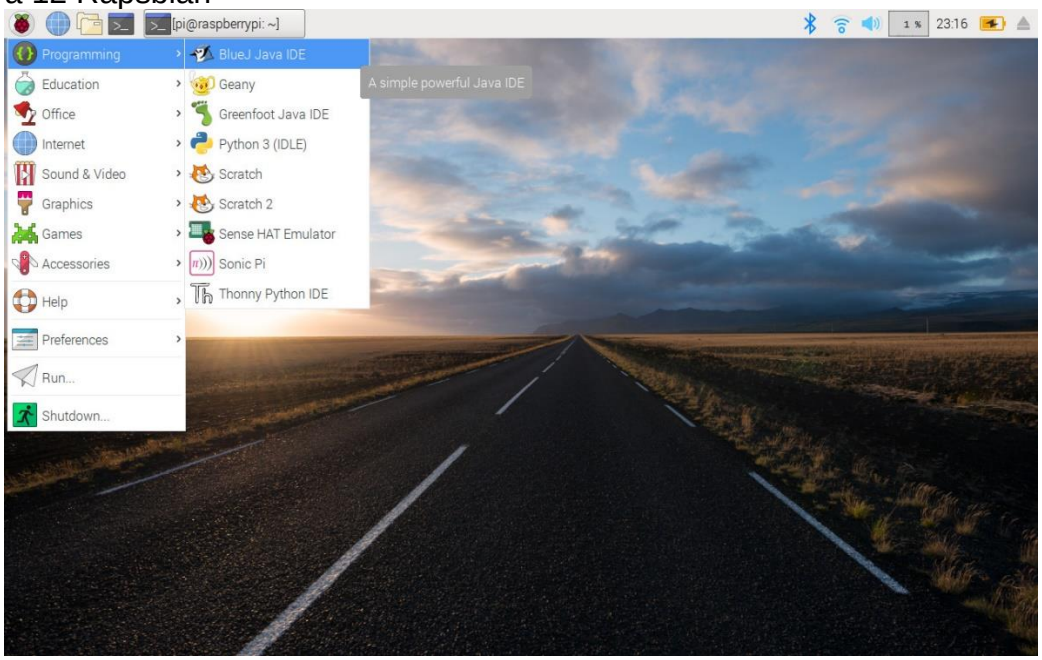
6.2.1. Distribuciones Linux orientadas a la programación

Raspbian

“Es un sistema operativo gratuito basado en Debian optimizado para el hardware Raspberry Pi. Un sistema operativo es el conjunto de programas básicos y utilidades que hacen que su Raspberry Pi funcione. Sin embargo, Raspbian proporciona más que un sistema operativo puro: viene con más de 35,000 paquetes, software precompilado incluido en un formato agradable para una fácil instalación en su Raspberry Pi[66]”.

[66] Taringa. [sitio web]. *Imagen SD de Raspberry Pi - Raspbian (sistema operativo Linux)*. [consulta: 16 de marzo 2020] Disponible en: https://www.taringa.net/chupinaybaila_2/imagen-sd-de-raspberry-pi-raspbian-sistema-operativo-linux_25lwtn.

Figura 12 Rapsbian



Fuente: Ubuntu. Install Ubuntu on a Raspberry Pi [Sitio web]. [Consulta: 22 de marzo de 2020].Disponible en: https://ubuntu.com/download/raspberry-pi

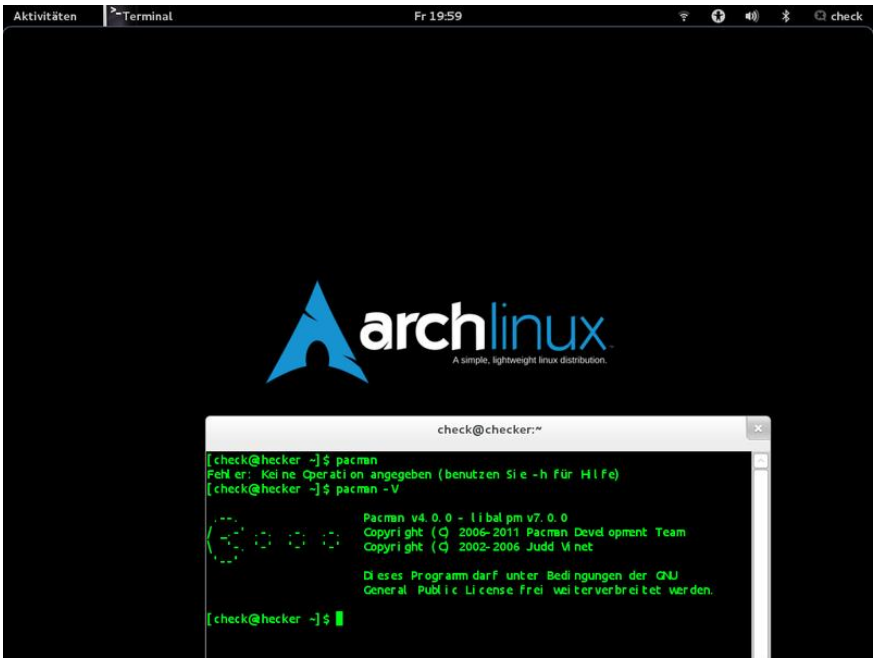
Características

- Incluye IDLE (herramienta de desarrollo para lenguaje Python y Scratch).
- Usa como escritorio LXDE y Midori como navegador web.
- Usa un entorno gráfico, el escritorio es LXDE, un escritorio libre de Unix al que se le denomina un Escritorio de Entorno Ligero.

Arch Linux

Es una distribución Linux para computadoras x86-644, arquitecturas ARM y I686 orientada a usuarios avanzados. Se compone en su mayor parte de software libre y de código abierto (FOSS)5 y apoya la participación comunitaria.6 Su modelo de desarrollo es de tipo Liberación continua[67].

[67] Linux en español. [sitio web]. *¿Qué es Arch? » Linux en español*. [consulta: 14 de abril del 2020] Disponible en: https://www.xn--linuxenespaol-skb.com/distribuciones/arch



Fuente: Archilinux. Arch Linux Downloads. [Sitio web]. [Consulta: 05 de abril de 2020].Disponible en: https://www.archlinux.org/download/

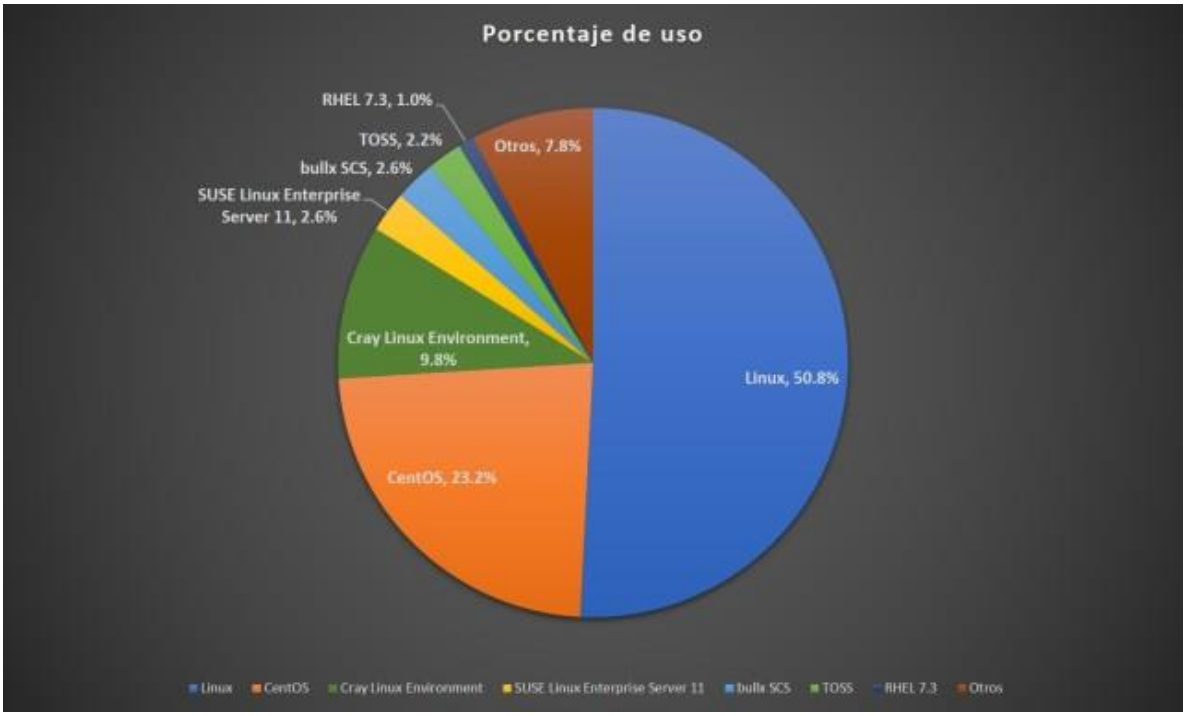
Características

- Carece herramientas de disposición intuitiva, dificultado su uso para usuarios finales sin conocimientos avanzados en Linux o llamados Slackware.
- Alto grado de niveles de conocimiento.
- No posee una plataforma promocional solo repositorios que puede ser compatibles con el sistema por lo cual dificulta su conocimiento.
- Arch Linux se basa en su manejador de paquetes, llamado Pacman. Solo se puede desarrollar mediante línea de comandos o terminal.

6.2.2. Distribuciones de Linux más usadas en laptops

La siguiente figura representa las versiones de Linux diseñada para computadores portátiles más usadas a nivel mundial.

Figura 14 Distribuciones que más se usan de sistemas operativos en supercomputadoras



Porcentaje de uso de sistemas operativos en supercomputadoras. Basado en datos de (PROMETEUS Professor Meuer Technologieberatung und -Services GmbH, 2018)

7. VULNERABILIDADES Y AMENAZAS EN DISTRIBUCIONES LINUX

En el siguiente capítulo abordaremos las vulnerabilidades y amenazas de las distribuciones de Linux no es un secreto de que la perfección no está en ninguno aspecto de la seguridad informática a tal punto de ser sistemas infranqueables por ello presentamos las diferentes flaquezas o debilidades de esta alternativa de sistema operativo como lo es Linux.

7.1. ESCALAMIENTO DE PRIVILEGIOS EN FREEBSD

"La localización de este agujero de seguridad se usa para beneficiar de la vulnerabilidad CVE-2013-2171, la cual accede hacer un generación de privilegios y permisos en FreeBSD (Sistema operativo). Quizá FreeBSD no sea el más conocido y público cuando se trata de máquinas de escritorio, por su compatibilidad de hardware, pero sí es suficiente utilizado cuando se trata de servidores"[68].

7.2. CVE-2014-3153 Detección de TowelRoot y exploits

"Es una vulnerabilidad PoC utiliza el hecho de que todas las aplicaciones y algunos servicios, incluido nuestro proceso malicioso, se bifurcan del proceso Zygote. Dado que todos sus procesos bifurcados heredan el mismo diseño de memoria, hace que la aleatorización del diseño del espacio de direcciones (ASLR) sea efectivamente inútil. Está vulnerabilidad bien explotada consentiría a un usuario local y sin permisos inhabilitar el kernel (el núcleo del sistema operativo) o inclusive remontar privilegios en el sistema"[69].

Descripción

"La implementación de la extensión BPF_S_ANC_NLATTR_NEST en la función sk_run_filter en net / core / filter.c en el kernel de Linux a través de 3.14.3 usa el orden inverso en una cierta resta, lo que permite a los usuarios locales causar una denegación de servicio (sobre-lectura y bloqueo del sistema) mediante instrucciones de BPF elaboradas. NOTA: el código afectado se movió a la función __skb_get_nlattr_nest antes de que se anunciara la vulnerabilidad"[70].

Versiones atacadas

- Metasploit, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, Mageia.

---

[68] WeLiveSecurity. [sitio web. *Amenazas para Linux: ¿cuáles son las que más se propagan y de qué tipo son?* | *WeLiveSecurity*. [consulta: 16 de marzo 2020] Disponible en: https://www.welivesecurity.com/la-es/2017/07/25/amenazas-para-linux-mas-se-propagan/

[69] Ibid.,

[70] Ibid.,

7.3. EREBUS

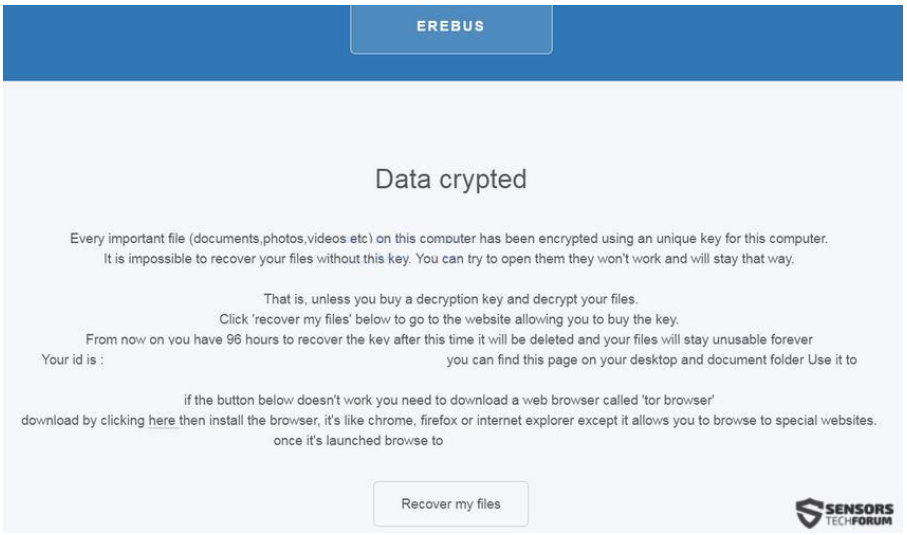
“Como es común en la mayoría de los ransomware, nació en un principio para infectar al sistema operativo Windows. Por entonces se distribuía mediante anuncios maliciosos (malvertising) que desviaban a las víctimas al kit de exploits Rig, utilizado para provocar la infección del ransomware. Esta variante de Erebus busca 423 tipos de ficheros y los cifra usando el algoritmo RSA-2048, además de añadir la extensión*. Encrypt* al final de estos. Tras investigar se descubrieron varios sitios web comprometidos que lo estaban difundiendo en Corea del Sur, los cuales estaban siendo utilizados como servidores de mando y control”[71]. (Medina, 2017)

“Erebus cambia de sistema operativo y ahora apunta a los servidores Linux. Utiliza el algoritmo RSA para cifrar las claves AES, cifrando los ficheros con claves AES únicas. Para permanecer en el sistema utiliza un falso servicio de Bluetooth para garantizar su inicialización incluso tras reiniciar el sistema y emplea una rutina cron para verificar cada hora la ejecución del malware. Debido a que el objetivo aquí son las empresas, el rescate en un principio era más alto, de 10 Bitcoints (24.689 dólares), aunque posteriormente bajó hasta los 5 (12.344 dólares). La variante de Erebus contra Linux infecta un total de 433 tipos de archivo (aunque Linux internamente no trabaja con extensiones como las de Windows), entre los cuales están pptx, docx, xlslx, sql, mbd, dbf, odb, zip, rar, eml, msg, html, css, php, java, avi y mp4. Erebus, el ransomware para Linux que está causando estragos a muchas empresas”.[72]

[71] MEDINA [sitio web], E. Erebus, el ransomware para Linux que está causando estragos a muchas empresas [Consulta: 19 de marzo del 2020]. Disponible en: https://www.muyseguridad.net/2017/06/26/erebus-ransomware-linux-empresas/

[72] MEDINA [sitio web], E. Erebus, el ransomware para Linux que está causando estragos a muchas empresas [Consulta: 19 de marzo del 2020]. Disponible en: https://www.muyseguridad.net/2017/06/26/erebus-ransomware-linux-empresas/

Figura 15 Ataque Ransomware Erebus



Fuente: Sensorstechforum. Nueva EREBUS Virus ransomware (Restaurar archivos).[Sitio web]. [Consulta: 09 de marzo de 2020]. Disponible en: https://sensorstechforum.com/es/new-erebus-ransomware-restore-files

8. . HERRAMIENTAS Y BENEFICIOS DE LAS DISTRIBUCIONES LINUX

En el capítulo anterior hablamos de las vulnerabilidades y amenazas en las distribuciones Linux que afecta a dicho sistemas operativos. En este capítulo tendremos en cuenta estas herramientas que ayudan a contrarrestar esas amenazas y generar seguridad en las distribuciones de Linux. A continuación presentaremos una serie de aplicación orientadas a la protección de la seguridad, integridad y operatividad de las distribuciones de Linux.

8.1. CLAMAV

El antivirus ClamAV es de código libre, es un eficaz rastreador virus y troyanos entre otras amenazas de seguridad y privacidad[73].

Características[74]

- compatible y ligero.
- Fácil de manejar.
- Detecta grandes cantidades de amenazas tales como gusanos y troyanos.
- Soporta arquitecturas de x64/x86 bit.
- Actualizaciones automáticas.
- Integración con Internet Explorer
- Soporte a Outlook

[73] Hup, B., [sitio web]. Install and update ClamAV antivirus for RSpamd anti spam - BenHup.com. [Consulta: 17 de septiembre 2019]. Disponible en: https://www.benhup.com/freebsd/clamav-antivirus-for-rspamd-anti-spam-install

[74] Hup, B., [sitio web]. Install and update ClamAV antivirus for RSpamd anti spam - BenHup.com. [Consulta: 17 de septiembre 2019]. Disponible en: https://www.benhup.com/freebsd/clamav-antivirus-for-rspamd-anti-spam-install

Figura 16 Entorno grafico ClamAV

Fuente: Malavida. ClamAV. [Sitio web]. [Consulta: 05 de junio de 2020]. Disponible en: https://www.malavida.com/es/soft/clamav/#gref

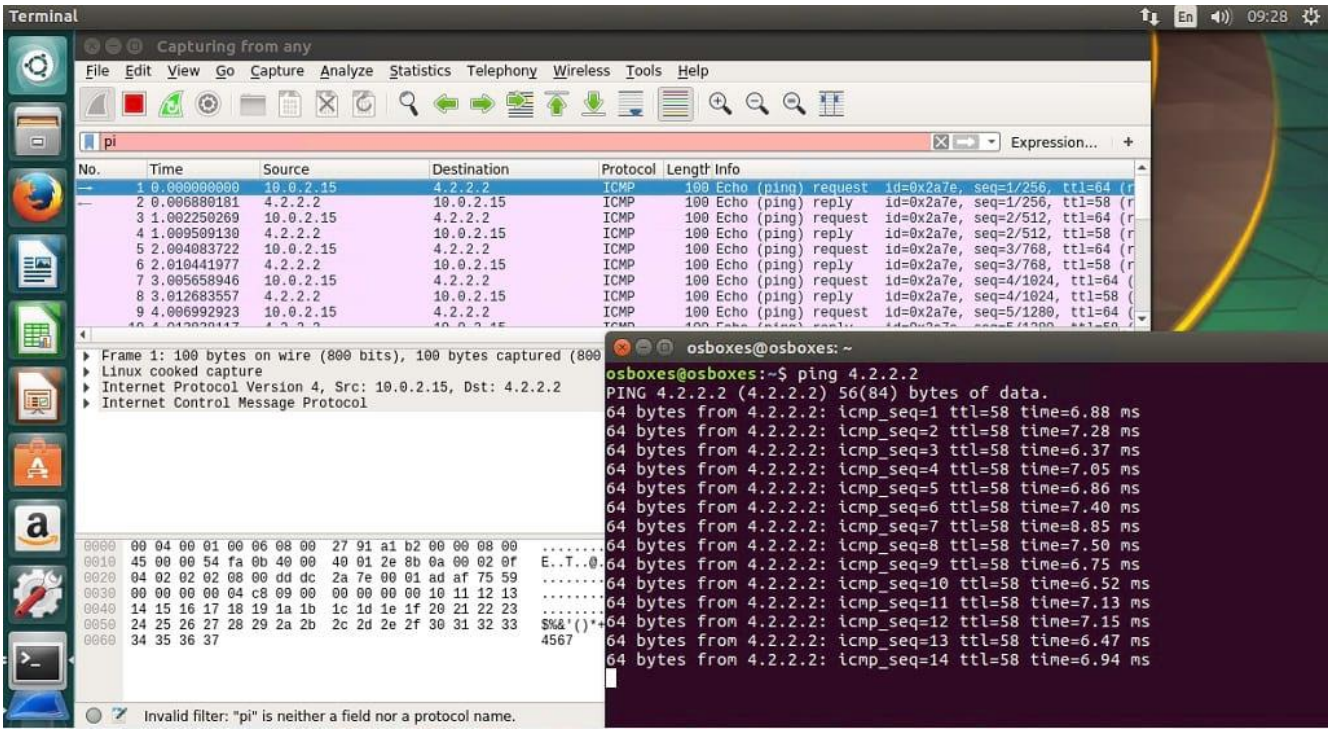
8.2. WIRESHARK

Es una popular utilidad multiplataforma de código abierto para el análisis de protocolos y paquetes de red[75].

Posee un amplio catálogo de análisis de VoIP, interfaz gráfica de usuario cómoda y análisis off-line, exportación a XML y muchas más funciones.

[75] Geekflare. [en linea]. *10 mejor software de monitoreo de código abierto para infraestructura de TI*. [8 de febrero 2021] Disponible en: <https://geekflare.com/es/best-open-source-monitoring-software/>

Figura 17 Herramienta WireShark en Kali Linux



Fuente: LinuxHint. Install Wireshark 2.4.0 – Network Protocol Analyzer on Ubuntu.[Sitio web]. [Consulta: 12 de septiembre de 2020]. Disponible en: https://linuxhint.com/install-wireshark-ubuntu-linux/

Ventajas de Wireshark[76]

- Su licencia es GPL.
- Muy completo.
- capturar datos de la red y exportación en archivo plano.
- librerías pcap.
- interfaz amigable.
- Gran capacidad de filtrado.
- Admite archivos tcpdump.
- Reconstrucción de sesiones TCP

[76] Solvetic. [sitio web]. *Herramientas gratis para monitorizar y analizar tráfico de red*. Consultado 8 de febrero de 2021]. Disponible en: https://www.solvetic.com/page/recopilaciones/s/seguridad/herramientas-gratis-monitorizar-analizar-trafico-de-red

- Multiplataforma.
- Usa múltiples protocolos (HTTP, HTTPS, TLS, TCP IP entre otros).
- Traductor de protocolos TCP IP.
- Crea SUX y TSM.

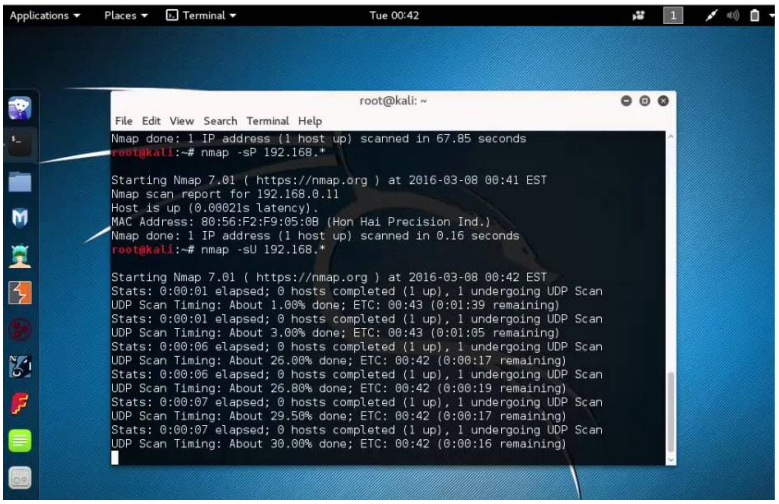
Desventajas

- No detecta intrusos.
- No maneja paquetes en la red.

8.3. NMAP

Es un programa dúctil, portable y de código libre para analizar redes y crear auditorías en seguridad. Sirve para gestionar los programas de actualización de servicios o la red y actividad monitorización tiempo real, etc[77].

Figura 18 Herramienta Nmap en Kali Linux



Fuente: ESTRADA. S. Osvaldo. NMAP comandos básicos en Kali Linux. [Sitio Web]. [Consulta: 22 de agosto de 2020]. Disponible en: http://osvaldosantiagoestrada.blogspot.com/2013/12/nmap-comandos-basicos-en-kali-linux.html

Características

[77] qdoc.tips. n.d. *Procesos y Herramientas Para La Seguridad de Redes - PDF Free Download*. [online] Available at: <https://edoc.pub/procesos-y-herramientas-para-la-seguridad-de-redes-pdf-free.html> [Accessed 8 February 2021].

- Detección de servidores: usando Ping para detectar computadores, máquinas virtuales y servidores por supuesto.
- Localización de back doors en computadoras.
- Detecta el sistema operativo usado y la versión de la computadora usada.

Ventajas

- Libre licenciamiento.
- Disponibilidad de acceder al código fuente.

Desventajas

- Complejo conocimientos sobre él.
- Nula documentación en línea.
- Ser autodidacta.

8.4. OSQUERY

Es una herramienta open source y usado en varias plataformas para el escaneo de redes e incidentes de seguridad. Es utilizado principalmente para ensayos periódicos de verificación de seguridad, descubrir fallas de memoria entre otras[78].

8.5. METASPLOIT FRAMEWORK

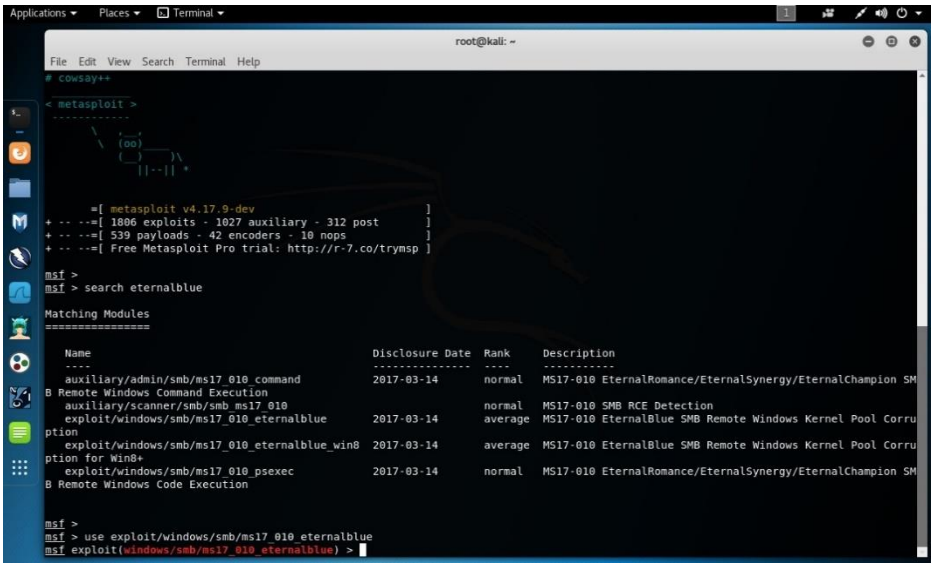
Se utiliza primordial y fundamentalmente para experimentos de penetración, pero también puedes utilizarlo para legitimar vulnerabilidades, realizar valoraciones de seguridad y mejorar tu conocimiento de seguridad para custodiar posibles atacantes[79].

---

[78] IBM Developer. [sitio web]. *Monitoring containerized environments with osquery*. [consulta: 17 de sep. 2019]. Disponible en: https://developer.ibm.com/technologies/containers/articles/monitoring-containers-osquery

[79] Ruby. [en línea]. *Metasploit Alternatives - Ruby Security | LibHunt*. [consulta: 23 de marzo 2020] disponible en: https://ruby.libhunt.com/metasploit-framework-alternatives

Figura 19 Herramienta Metasploit en Kali Linux



Cyberdefenders. Kali Linux & Metasploit: Getting Started with Pen Testing. [Sitio web]. [Consulta: 04 de junio de 2020]. Disponible en: https://medium.com/cyberdefenders/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b

Ventajas de Metasploit

- Multiplataforma y gratis, aunque tiene una versión de pago, es costosa.
- Accede interactuar igualmente con funciones externas, como Nmap o Nessus.
- Suministra una interfaz apoyada en consola con el Framework Metasploit.

Desventajas de Metasploit

- Solo es mejora ocasionalmente.
- Práctica, pero da una carga excesiva a la memoria de la maquina
- No administra en lo imperioso nada de seguridad, y solo se debe usar en redes de seguridad.

9. CONCLUSIONES

Una vez concluido el estudio monográfico podemos concluir lo siguiente

- La variedad de distribuciones de Linux que están disponible para diversos propósitos o multitarea si es necesario.

- Comercialmente es favorable a diferencia de sus otros competidores por ende el uso de Linux debido a su política y filosofía Opensource y en algunas ocasiones copyleft lo que incentiva más su uso.

- Cuenta con una comunidad que respalda su versionamiento y funcionamiento de sus diferentes distribuciones.

- Aunque cuente con ataques como cualquier sistema operativo del mercado cuenta con muchas diferencias desde su instalación de software en sus distribuciones.

- Sus herramientas son totalmente free (libres) pero encontrar documentación es extremadamente difícil solo se ciñe a la documentación oficial.

10. RESULTADOS

- Como resultado de esta monografía tenemos mucho para analizar en termino de números de distribuciones y familias de Linux que contribuyeron a la elaboración y construcción de mi monografía como trabajo de grado empezamos enumerando las 3 distribuciones de Linux orientadas a la seguridad o pentesting (**Kali Linux, Openwall y Subgraph OS**), a las distribuciones enfocadas a servicios de firewall (**ClearOS y Smoothwall**) a las distribuciones derivadas al análisis forense y auditoria(**BackBox y Santoku Linux**) distribuciones enfocadas al ámbito empresarial y servidores (**Red Hat Enterprise Linux, SUSE Linux Y Ubuntu Server**) y por ultimo orientada a smartphone(**Firefox OS, Android y Tizen**) para contar un total de 13 distribuciones Linux que se encargan específicamente de una funcionalidad lo cual es el objetivo principal de esta monografía.

- Existen muchas herramientas Opensource orientada a Linux que facilitan el escaneo de vulnerabilidades, detección de amenazas, detección de intrusos, exploit y demás, para ello dentro de muchas herramientas sean tenido en cuenta aplicaciones con ClamAV, WIRESHARK, NMAP, METASPLOIT que permiten realizar todo tipo acciones para contrarrestar las diferentes ataques que están dirigidos a las plataformas Linux.

- También podemos destacar dentro de los resultados las 3 vulnerabilidades más frecuentes que presentan las distribuciones Linux como también las diferentes herramientas que cuenta para contrarrestar dichas amenazas.

11. RECOMENDACIONES

- Linux como sistema operativo presentan muchas variantes y múltiples distribuciones para su uso, pero debes tener en cuenta que para usar las distribuciones de Linux debes conocer la necesidad personal u organizacional que requieras para utilizar dicha distribución documentarse bien sobre su instalación, uso y prestación que le pueda dar a tu necesidad para cumplirla.

- Recuerda las distribuciones de Linux no tiene ningún valor comercial debido a su política o filosofía de uso libre.

- Es necesario tener amplios conocimientos sobre Linux debido a que su documentación es muy escasa o solo se encuentra en sitio oficiales debido a que muchas de las distribuciones no son muy populares.

12. BIBLIOGRAFÍA

12 CARACTERÍSTICAS [sitio web]. 12caracteristicas [consulta: 20 de marzo 2020].Disponible en: https://www.12caracteristicas.com/debian/

Hardening. [Sitio web]. [Fecha de consulta 7 febrero 2021] disponible en: https://hardeningpatching.weebly.com/hardening.html

Arquiñano, c. [Sitio web]. Seguridad Informática Mc Graw-Hill [Sitio web]. [Fecha de consulta 7 febrero 2021] disponible en: https://www.academia.edu/8358689/Seguridad_Informatica_Mc_Graw_Hill_2013_www_Free_Libros_me_copia

José Romero, C. [Sitio web]. Sistema Operativo LINUX. [Fecha de consulta 7 febrero 2021] disponible en https://sistemaoperativolinuxune.blogspot.com/

Albornoz, L. [Sitio web]. El riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas BASC. [Fecha de consulta 7 febrero 2021] disponible en: https://www.academia.edu/28646328/El_riesgo_y_la_falta_de_pol%C3%ADticas_de_seguridad_inform%C3%A1tica_una_amenaza_en_las_empresas_certificadas_BASC

SISTEMAS, A. [Sitio web]. AUDITORIA DE SISTEMAS. [Fecha de consulta 7 febrero 2021] disponible en: https://portafolioauditoriasistemas.blogspot.com/2009/04/

Pérez Hernández, M., & Duarte, A. La informática, presente y futuro en la sociedad, Córdoba: El Cid Editor. 2006, p. 1

ARENA, H. Linux avanzado. Buenos Aires: MP Ediciones.2000

Martínez, S. [Sitio web]. INTRODUCCION A LA INGENIERIA DE SISTEMAS. [Fecha de consulta 7 febrero 2021] disponible en:https://www.academia.edu/24927405/INTRODUCCION_A_LA_INGENIERIA_DE_SISTEMAS

Mancilla, j. [Sitio web]. JUAN CARLOS BACCA MANCILLA. [Fecha de consulta 7 febrero 2021] disponible en: https://juancarlosbaccamancilla.blogspot.com/

Cesar A. Duque A y Asociados Consultores de riesgos. Metodología para la Gestión de Riesgos [en línea] pág. 1-9 [2001] [consulta: 14 de abril 2020]. Disponible en: http://www.ridsso.com/documentos/muro/207_1469148692_57916e1488c74.pdf

DEBIAN. [Sitio web]. Acerca de Debian, [consulta: 9 de marzo de 2020]. Disponible en: https://www.debian.org/intro/about

Alamanni, M. Kali Linux Wireless Penetration Testing Essentials. BIRMINGHAM, REINO UNIDO: Packt, 2015. Pag 55-61 ISBN 9781119323983

ANDRÉS CHÁVEZ. [Sitio web] Capítulo 1 - Conceptos Básicos Networking, consultado [20 de marzo 2020] Disponible en: https://www.academia.edu/24349658/Conceptos_b%C3%A1sicos_de_Networking

Seguridad Informática [Anónimo].Capítulo 2 - Seguridad Informática. Pag 36-57

ANTONIO, L. Ventajas & Desventajas De Linux Ubuntu [sitio web]. Obtenido de Ventajas & Desventajas De Linux Ubuntu [consulta: 22 de marzo de 2020]. Disponible en: http://loganventajasydesventajasubuntu.blogspot.com/

Barzanallana, R. Introducción a la Seguridad Informática. Obtenido de Gestión de la Seguridad en Sistemas de Información [en línea]. Tesis, universidad de Murcia, 2017 consultado [22 de marzo de 2020] disponible en: https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf

Basaldua, L. D. Tesis Seguridad en Informática (auditoria de Sistemas) (2005). México.

BLOGSPOT. [Sitio web]. Instalación, características, ventajas y desventajas del sistema operativo Linux Ubuntu server, desarrollado por canonical LTD [19 de 09 de 2019]. Disponible en: http://isft179-ubuntuserver.blogspot.com/

Catarina. . [Sitio web]. Capítulo 1 - seguridad informática - conceptos básicos [19 de 09 de 2019]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf

CDM [sitio web]. Historia de Linux [19 de 09 de 2019]. Disponible en: http://www.cad.com.mx/historia_de_linux.htm

CENTOS. [Sitio web]. Preguntas frecuentes sobre CentOS en general. [Consulta: 12 de septiembre de 2019] disponible en: https://wiki.centos.org/FAQ/General#head-4b2dd1ea6dcc1243d6e3886dc3e5d1ebb252c194

Central, P. E [sitio web] [2015]. [Linux avanzado 2a. ed. Editorial ICB].

CLEARFOUNDATION. [Sitio web]. Claros [Consulta: 09 de mayo de 2019]. Disponible en: https://www.clearos.com/clearfoundation/software/clearos-7-community

Colombia. [Sitio web] congreso de Colombia. Ley 87 (29 de noviembre de 1993). Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones. Disponible en: https://www.mininterior.gov.co/sites/default/files/ley_87_de_1993.pdf

Colombia. [Sitio web] congreso de Colombia. Ley 603 de 2000 [27 de julio de 2000]. Por la cual se modifica el artículo 47 de la Ley 222 de 1.995. Disponible en: [http://derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307]

Colombia. [Sitio web] congreso de Colombia. Ley 594 de 2000 [14 de julio de 2000]. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Disponible en: [https://www.mintic.gov.co/portal/604/articles-15049_documento.pdf]

Colombia. [Sitio web] congreso de Colombia. Ley 734 de 2002 [5 de febrero de 2002]. Por la cual se expide el Código Disciplinario Único. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0734_2002.html

Colombia. [Sitio web] congreso de Colombia. Ley 1266 de 2008 [19 de junio de 2019]. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Colombia. [Sitio web] congreso de Colombia. Ley 1581 de 2012 [15 de junio de 2019]. Por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Colombia. [Sitio web] congreso de Colombia. Ley 527 de 1999 [15 de junio de 2019]. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

COMUNICACIONES [sitio web] Manual de Normas y Políticas de Seguridad Informática [consulta: 24 de septiembre de 2019]. Disponible en:

https://www2.sgc.gov.co/ControlYRendicion/TransparenciasYAccesoAlaInformacion/CircularesManuales/MO-TEC-001-I.pdf

Conocimiento Libre. [Sitio web]. 10 nuevas características en Ubuntu 19.04 Disco Dingo - Conocimiento Libre. [Consulta: 24 de septiembre de 2019] disponible en: https://conocimientolibre.mx/ubuntu19-04-caracteristicas

CSIRT-cv. (s.f.). 12 medidas básicas para la seguridad Informática. Valencia: Generalitat Valenciana.

DACCACH [sitio web] Ley de Delitos Informáticos en Colombia [consulta: 23 de marzo 2020]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Debian.org. 2021. Debian -- About Debian. [En linea] [8 febrero 2021]. Disponible en: https://www.debian.org/intro/about

Digitales, T. Estructura y funcionalidad de un sistema de seguridad informática (2017). Puebla México: Universidad de las Américas.

DISTROWATCH [Sitio web]. Noticias, enlaces, información y actualización, ranking de popularidad, Software [consulta: 14 de abril del 2020]. Disponible en: https://distrowatch.com/?language=ES

DocPlayer. (s.f.). Capítulo 1.- Marco teórico. Obtenido de https://docplayer.es/3553490-Capitulo-1-marco-teorico.html?cv=1

E-boom, P. (2015). Linux avanzado (2a. ed.), En Linux avanzado (2a. ed.), Editorial ICB.

ECURED [Sitio web]. Firefox OS [consulta: 14 de abril del 2020]. Disponible en https://www.ecured.cu/Firefox_OS#.C2.BFQue_es_Firefox_OS.3F

Ecured.cu. 2021. Santoku Linux - EcuRed. [En linea] [8 Febrero 2021]. Disponible en: https://www.ecured.cu/Santoku_linux.

Ediciones-eni.com. [sitio web]. Libro Android - Guía de desarrollo de aplicaciones Java para Smartphone y Tabletas (3ª edición). Disponible en: https://www.ediciones-eni.com/libro/android-guia-de-desarrollo-de-aplicaciones-java-para-smartphones-y-tabletas-3-edicion-9782409006104.

Escrivá, G. G. Seguridad informática. Macmillan Iberia, S.A. 2013

GREENBERG, A [sitio web]. Whonix [consultado: 17 de marzo de 2017]. Disponible en: https://www.whonix.org/

Geekflare. [En linea]. 10 mejor software de monitoreo de código abierto para infraestructura de TI. [8 de febrero 2021] Disponible en: <https://geekflare.com/es/best-open-source-monitoring-software/>

HERNÁNDEZ, P. F. Sistema operativo Windows: presente y futuro. [En linea] 2006. Pag 121-157 ISBN 978-607-02-6544-0 .disponible en: https://libros-revistas-derecho.vlex.es/vid/sistemas-operativos-445312738

IBÁÑEZ.H [sitio web].Sistemas operativos [consulta: 17 de septiembre 2019]. Disponible en: https://www.monografias.com/trabajos11/opera/opera.shtml
Hup, B., [sitio web]. Install and update ClamAV antivirus for RSpamd anti spam - BenHup.com. [Consulta: 17 de septiembre 2019]. Disponible en: https://www.benhup.com/freebsd/clamav-antivirus-for-rspamd-anti-spam-install

IBM Developer. [Sitio web]. Monitoring containerized environments with osquery. [Consulta: 17 de sep. 2019]. Disponible en: https://developer.ibm.com/technologies/containers/articles/monitoring-containers-osquery

Holguín, L., [en linea]. Sistema Operativo Centos. [Consultado: 8 Febrero 2021] Disponible en: https://luisa-holguin19.blogspot.com/2012/06/.

JULIÁ [sitio web]. Gadae [consulta: 17 de septiembre 2019]. Disponible en: http://www.gadae.com/blog/ventajas-utilizar-linux/

LINUX [sitio web], S. SuSE, [consulta: 14 de abril del 2020]. Disponible en: https://www.suse.com/es-es/products/realtime/technical-information/

Linux en español. [Sitio web]. ¿Qué es Arch? » Linux en español. [Consulta: 14 de abril del 2020] Disponible en: https://www.xn--linuxenespaol-skb.com/distribuciones/arch

LÓPEZ, JOSÉ MARÍA [sitio web]. Linux, seguridad y análisis forense digital [consulta: 25 de marzo de 2020]. Disponible en: https://hipertextual.com/2018/12/linux-seguridad-analisis-forense-digital

MACÍAS-VALENCIA, S. M.-Z. Seguridad en informática [en linea] 2017: consideraciones. Revista Científica: Dominio de las Ciencias, 3(4), 13.

MARTHA IRENE ROMERO CASTRO, G. L. Introducción a la seguridad informática y el Análisis de Vulnerabilidades [en linea] 2018. Pag 53-79 ISBN 8494930613 disponible en:

https://books.google.com.co/books/about/INTRODUCCI%C3%93N_A_LA_SEGURIDAD_INFORM%C3%81TIC.html?id=5Z9yDwAAQBAJ&source=kp_book_description&redir_esc=y

MARTIN MEREDITH, N. P. [sitio web]. Techradar [consulta: 19 de septiembre del 2019]. Disponible en: https://www.techradar.com/best/best-free-linux-firewalls

MARTIN MEREDITH, NICK PEERS, NATE DRAKE, BRIAN TURNER [sitio web]. 6 best free Linux firewalls of 2017. [Consulta: 19 de marzo del 2020]. Disponible en: https://www.techradar.com/best/best-free-linux-firewalls

MARTÍNEZ, J. A [sitio web]. La empresa ante el software libre [Consulta: 19 de marzo del 2020]. Disponible en: http://es.tldp.org/COMO-INSFLUG/COMOs/La_empresa_ante_el_software_libre/

MEDINA [sitio web], E. Erebus, el ransomware para Linux que está causando estragos a muchas empresas [Consulta: 19 de marzo del 2020]. Disponible en: https://www.muyseguridad.net/2017/06/26/erebus-ransomware-linux-empresas/

Mocq-librosvirtual, R., [sitio web]. Raspberry Pi 3 O Pi Zero - François Mocq-librosvirtual [Consulta: 19 de marzo del 2020]. Disponible en: https://idoc.pub/documents/raspberry-pi-3-o-pi-zero-franois-mocq-librosvirtual-x4e6193xm3n3

López, M., [en linea]. Seis distribuciones de Linux enfocadas a empresas. [Consultado 8 de febrero de 2021] Genbeta.com. Disponible en: https://www.genbeta.com/linux/seis-distribuciones-de-linux-enfocadas-a-empresas.

MIRANDA. J [sitio web], Breve historia de Linux [10 de marzo de 2020]. Disponible en: http://www.iuma.ulpgc.es/users/jmiranda/docencia/libro_ada/libro_ada_html/node133.htm

MoinMoin [anónimo]. Disponible en: https://www.raspbian.org/

OS, S. [sitio web]. Subgraph OS Adversary resistant computing platform [consulta: 17 de octubre de 2019].Disponible en: https://subgraph.com/sgos/

Padilla, M. S. Análisis y Riesgos de la información. Revista Killkana (mayo - agosto de 2017).

QUIROZ, S. M. Seguridad informática. Consideraciones en Revista Científica Ciencias, 2017 pp.676-688. Científica Ciencias, 3(5), 676-688. .ISSN:2477-8818.Vol 3, núm. 5

RAÚL J. MARTELO. Modelo Básico de Seguridad Lógica [en línea] 2018. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia pág 16-20. ISSN 0718-0764. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003&lng=en&nrm=iso&tlng=en

REDESZONE [sitio web]. ¿Cuál es la mejor distribución Linux para usar en servidores? [03 de marzo de 2019]. Obtenido de https://www.redeszone.net/2019/03/03/mejor-distro-linux-servidores/

ROMERO, I., FIGUEROA, G. L., VERA, D., ALAVA, J., MURILLO, A., & & CASTILLO, M. Introducción a la seguridad informática y el Análisis de vulnerabilidades. [En linea] 2018 3. Ciencias-Editorial área de innovación y Desarrollo. Universidad Estatal del Sur de Manabi. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Roshy.net. [sitio web]. Ubuntu, un OS para todos – cursos roshy. [8 de feb. de 2021] Disponible en: http://roshy.net/sistemas/2019/03/29/ubuntu-un-os-para-todos

ROSERO, J. H. Implementación de software educativo libre en la institución educativa nuestra señora de Lourdes [en línea] proyecto de grado. Universidad de Nariño. 2007. [consulta: 23 de marzo 2020] disponible en: http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/73193.pdf

Ruby. [en línea]. Metasploit Alternatives - Ruby Security | LibHunt. [consulta: 23 de marzo 2020] disponible en: https://ruby.libhunt.com/metasploit-framework-alternatives

SÁNCHEZ, K. G. Tesis Análisis en seguridad informática y seguridad de la información (marzo de 2015). Basados en: la norma ISO/IEC 27001

SEGURIDAD [sitio web] open Wall [Consulta: 19 de marzo del 2020]. Obtenido de https://www.openwall.com/Owl/

Senado, Senado de la república. Ley 1273 de 2009 (13 de mayo de 2019). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Senado de Colombia, Senado de la república. Ley 599 de 2000 (15 de junio de 2019). Por la cual se expide el Código Penal. Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

SERVER [sitio web], S. L. SUSE Linux Enterprise Server [15 abril 2019].Disponible en: https://documentation.suse.com/sles/15-SP1/

Sistemas Operativos 2017-1. [Sitio web], Tizen. [Consulta: 16 de marzo 2020] Disponible en: https://chsosunal20171911005.wordpress.com/2017/05/22/tizen/.

STELLA RODRÍGUEZ, G. El software libre y sus implicaciones jurídicas [en linea] 2008 pág. 1-7 [consulta: 16 de marzo 2020] ISSN 0121-8697. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000200007

Solvetic. [Sitio web]. Herramientas gratis para monitorizar y analizar tráfico de red. Consultado 8 de febrero de 2021]. Disponible en: https://www.solvetic.com/page/recopilaciones/s/seguridad/herramientas-gratis-monitorizar-analizar-trafico-de-red

Taringa! [Sitio web]. Imagen SD de Raspberry Pi - Raspbian (sistema operativo Linux). [Consulta: 16 de marzo 2020] Disponible en: https://www.taringa.net/chupinaybaila_2/imagen-sd-de-raspberry-pi-raspbian-sistema-operativo-linux_25lwtn.

WeLiveSecurity. [Sitio web. Amenazas para Linux: ¿cuáles son las que más se propagan y de qué tipo son? | WeLiveSecurity. [Consulta: 16 de marzo 2020] Disponible en: https://www.welivesecurity.com/la-es/2017/07/25/amenazas-para-linux-mas-se-propagan/

WIKIDOT [sitio web]. Seguridad Informática [consulta 26 de marzo de 2020]. Obtenido de http://seguridadinformatica.wikidot.com/seguridad-informatica